Microsoft 365 (M365) Project Rollout Review

Assignment Report 2022/23 (Final)

Cheshire Fire and Rescue Service (Fire Service)

Report Ref: 302CFRS_2223_901

Date of Issue: 27th June 2023

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	20th March 2023
Discussion Meeting	Online - May 2023
Final Draft Report Issued	May 2023
Client Approval Received	27th June 2023
Final Report Issued	27th June 2023

Report Distribution

Name	Title
Alex Waller	Chief Fire Officer and Chief Executive
Lee Shears	Deputy Chief Fire Officer
Andrew Leadbetter	Director of Governance and Commissioning
Paul Vaughan	Treasurer / Audit Lead
Pete Hayes	Project Manager – M365
Stuart Rogers	Head of IT / Chief Information Security Officer (CISO)
Neil McElroy	Head of Service Improvement
Graham Foster	Head of Technical Operations
Chris Astall	Planning, Performance and Risk Officer
Emma McDonough	Governance and Assurance Manager

Audit Team

Name	Contact Details	
Catherine Watts	catherine.watts@miaa.nhs.uk	07554 338 496
Paula Fagan	paula.fagan@miaa.nhs.uk	07825 592 866
Anne-Marie Harrop	Anne-marie.harrop@miaa.nhs.uk	07710 229471

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 review was conducted in accordance with the requirements of the 2022-23 Internal Audit Plan, as approved by the Audit Committee.

Cheshire Fire & Rescue Service (Fire Service) were continuing to rollout Microsoft 365 (M365) across their estate, having worked with external third parties, such as Insight / Comms-care to implement and test the initial deployment. This is seen as a key connectivity and collaborative solution going forward for the Fire Service. They were keen to continue maturing the solution and embedding it within the service governance and control framework.

A programme of work of this magnitude is inherently risky and challenging and a variety of governance and control processes are necessary to provide management with assurance that the programme is on track and that risks, issues and challenges are being appropriately managed.

This system implementation presents a significant investment and change for the Fire Service not only operationally but culturally due to the nature of the new system, allowing more collaborative working going forward. Senior management within the Fire Service recognised the importance of having appropriate controls in this area and therefore commissioned this review.

1.2 Opinion

Limited Assurance	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.

1.3 Key Findings

Overall, the review identified that controls were not operating effectively and required improvement to ensure consistent and affective application. The Fire Service were deploying MS Teams and OneDrive functionality as part of an initial pilot and then deploying this functionality across the estate. Off-boarding the pilot project to business-as-usual was not a formally defined phase of the project plan, with roles and responsibilities to be confirmed. Also. use case modelling had not been undertaken to baseline the project.

It was noted too that threats to passwords have continued to rise, inflating the level of risk, and requiring further actions to be taken by organisations. Examples of such attacks include password spraying attacks, which target numerous accounts with commonly used / weak passwords and the targeting of key individuals / privileged accounts. However, while several security policies had been configured, not all were enabled, and enforced. For instance, emails were currently accessible from personal devices, users could copy web mails to their desktop and send personal emails to shared folders.

In addition, regular staff training such as through phishing exercises should be undertaken and business continuity plans published and tested.

This review was commissioned by the project team to better understand the controls in place and identify areas where controls could be introduced / strengthened. New solutions / skills / features need to be matured and embedded within the organisation and this will take time and appropriate strategy.

The following provides a summary of the key themes.

Sub Objective	Key Themes
Technical controls and resilience, and recovery arrangements including security incident reporting Hybrid based - host infrastructure, location, and technical controls And Resilience and recovery arrangements And Security Incident Reporting	Areas of good practice: • We were advised that the tenant used the National Enabling Programmes (NEP) Design blueprint used by the Police Service to configure the tenant and worked with the third-party Comms Care – InSight. • Email was to be using Transport Layer Security (TLS) v1.2 encryption by default. • Alerts and suspicious activity were being reported to the Police IT Security team. The Police IT Security team had privileged accounts / administrator accounts on premise and requests for privileged accounts were managed through them / were subject to formal approval. • We were advised that laptops were updated in May / June 2022, with the upgrade taking 3 months. 40 mobile phones had been purchased and Net Motion now provided Wi-Fi connectivity instead of Cisco. • The IT team were moving public folders to exchange online and upgrade mobile phones to work with InTune. IT had established a security group to enable Sway and stream for a limited number of users in the training department. • A risk around the MS query tool impacting key reporting performance was raised / being tracked. Users were using virtual machine “pools” for Fire / Police services whilst the Azure virtual desktop was under development. Areas for improvement • Although the tenant was implemented in line with the NEP blueprint there were weaknesses, exceptions and anomalies on the estate. For instance, technical controls such as Bit Locker and InTune were not implemented across all the estate and users were using virtual machine “pools” for Fire / Police services. We were advised that 4 solutions were currently under investigation and 4 people, including those in the performance and planning team, would be impacted if access to these services was removed. Additional work was needed to ensure Fire Services operated as expected on M365. • Work in progress included M365 moving to exchange online with user mailboxes, and the home shared drive was to be

Sub Objective	Key Themes
	migrated off premise to OneDrive in April 2023, and then personal drives would be made read-only. - Business continuity plans were not documented, approved, published and tested.
Strategy for information protection and security management. Strategy for information protection. And Strategy for security management such as use of dashboards, and audit and logging, threat protection and identify and access controls.	Areas of good practice: - Conditional access policy was evidenced showing policies had been established to enforce two factor authentication for all users bar the "break-glass" account. Lockdown settings included logging, log on / account management events, 5 passwords being remembered, 10-character passwords with complexity enabled, a lockout for 10 minutes and 5 invalid attempts. However, see Areas for improvement. - IT provided a screenshot of the guest settings (only users assigned specific administrator roles can invite guests) with no users assigned the guest inviter Azure Active Directory role so no guests can be added to the tenant. - An audit log example was provided showing how user activity could be logged and reviewed, - Evidence of a Teams meeting recording having expired and being deleted, and an associated notification to the user was provided. Areas for improvement - A strategy for managing data retention / cleansing data was not agreed although data stored on MS Teams could be requested for a relevant Freedom of information (FOI) or Subject Access Request (SAR). - Plans to enforce stricter controls were underway however, the functionality was not yet available. Controls were not subject to ongoing compliance and monitoring. - Although data policies had been configured, these were not currently enabled / enforced. For instance, emails were currently accessible from personal devices, users can copy web mails to their desktop and send personal emails to shared folders. Security configurations should be enabled and subject to a regular assurance regime. - The organisation should review / confirm that all accounts now have Multi Factor / Two Factor Authentication (MFA/ 2FA) deployed as planned and include this check as part of ongoing compliance checking.

Sub Objective	Key Themes
	• Azure Information Protection, as part of the Microsoft Purview solution had not been enabled to discover, classify, protect, and govern sensitive information where it resides or travels. • A solution for searching mailboxes to support investigations was currently not available. • Training of staff about the increased threats of phishing emails, such as through regular phishing exercises was not scheduled and performed as part of an assurance regime.
Information governance, risk management, and roles and responsibilities. Information governance and risk management . And Roles and responsibilities including administration and staff training.	Areas of good practice: • Key departments for the pilot had been identified and agreed and a key sponsor for the pilot assigned for the project, however, see Areas for improvement. • A risk and issues register (RAID) for M365 were evidenced. • Senior Management Team (SMT) reports for M365 – revised approach and implementation progress update (14/2/22 final) were provided as well as an end of pilot user testing and sign off to move into a wider roll (out) were provided. Areas for improvement • We were advised that a risk management group was due to recommence at the end of Jan. 23 and a Member Project Board had been meeting sporadically. The organisation should reinstate appropriate group(s) to oversee the project and consider its controls. • Policies to underpin system requirements were not subject to compliance monitoring and assurance reporting. • We were advised that a Teams Lite Data Privacy Impact Assessment (DPIA) was in draft. It should detail a clear data strategy to ensure appropriate usage, control, and management of the M365 applications and data. • An Information Asset Owner (IAO) and project manager for the Fire Service to oversee and manage the business-as-usual activities were to be confirmed. • An assurance regime, including penetration test date was not scheduled and approved.
Use cases for the Office 365 applications.	Areas of good practice: • We were advised that the service brought in Valto Microsoft IT Services in Mar. / Apr. 2022 to provide recommendations

Sub Objective	Key Themes
	around business change and inform an overarching strategy for MS Teams. - The licensing model was a mixture of E3 and some E5 functionality. The use case for purchasing licences was originally per device and not per user, however, during the rollout it was identified that extra licences were required, and these licences were subsequently purchased. - The Fire Service had run MS Teams and Skype in parallel with Skype support due to end in March 2023. A decision had been made to remove Skype. - The project team had identified 100 of the 500 mailboxes as shared mailboxes. We were advised that they migrated 28 mailboxes during Dec. 2022 and upgraded 17 successfully. Another 37 were being migrated during 30th Jan. – 31st Mar. 2023. Phone upgrade guidance including advising staff to save mobile phone contacts was evidenced. - The Police IT Service managed any day-to-day mailboxes issues and / or recovery of items through their service desk. Areas for improvement - Analysis of departments and best deployment use case scenarios were not formalised and agreed. No use case modelling was provided and as a result gaps in controls were identified within this report. - For example, shared mailboxes / legacy mailboxes were not originally identified as part of the project requirements. These requirements required further modelling. - During the rollout it was discovered that MS Teams resulted in increased data usage costs as users accessed Teams via mobile devices using data by default rather than Wi-Fi. Going forward data usage should be part of the use case modelling.
Up to date plans, policies, and procedures in place for delivery, maintenance, and compliance.	Areas of good practice: - A project manager had been appointed by the Fire Service and a Project Initiation Document (PID) produced (July 21). - The methodology adopted was a waterfall of mini project phases. The project plan included the following phases, implement Teams lite, migrate shared (h) drive to OneDrive, migrate to M365 virtual instance (similar to the Police Service), mailbox migration and phone upgrade, and then

Sub Objective	Key Themes
	Azure virtual desktop. However, see Areas for improvement. - A statement of work was being confirmed for the Azure virtual desktop work. - Teams' guidance, OneDrive setup guidance and a two-factor authentication briefing guide were evidenced. Planner form functionality and training were also being published for the communications team to perform surveys. Process documents for starters, movers and leavers were also evidenced. - M365 updates were being published via Alert magazine, Green magazine, and the intranet. Direct emails were also sent to specific groups. - A PowerPoint produced in Jan. 2023 to provide an update report on the project was evidenced. - Training had been provided online through clinics, hosting 5-6 people. 4 clinics had been run in total. Going forward additional drop-in clinics were to be offered. Areas for improvement - Off-boarding the pilot project to business-as-usual was not a formally agreed phase as part of the project plan. - A technical road map for future functionality / maintaining current controls was to be documented and the associated risks / issues for the next phase required a refresh. - Further guidance / training was planned to enhance the intranet documentation. For instance, guidance was to be added about how to set up public / private channels.
Change control and support arrangements	Areas of good practice: - The Fire Service had awarded a contract to Insight directly. Service Level Agreements (SLAs) with M365 were as per the online SLAs and were not customised. - The Fire Service had purchased 880 Enterprise Agreement licences for E3, with Enterprise Mobility and Security E3, and Microsoft 365 E5 Security. By default Sway and Project were not available and Project required additional licencing. - The police service provided IT resource, cyber security expertise and a strategic change team. IT change control was managed through the Police IT service desk.

Sub Objective	Key Themes
	- Weekly meetings were taking place to discuss changes between the Project Manager / IT. Request for Change (RFC) examples were provided (257800, 253309, 250604 and235702) with RFC 260645 the go live approval for M365, enabling IT to migrate the remaining mailboxes / upgrade the phones to InTune by the end of March 2023. Change notes had been filed by the Project Manager. - Knowledge articles were provided through the IT service desk. User guidance and staff communication were also being produced by the project manager. - A Change Management policy (v2.5 / Issued 4/12/20) was provided and a post deployment validation and acceptance spreadsheet evidenced. - The Police IT service catalogue Alemba outlined the service (M365 / Teams / Email) along with tier type, SLA, respond and fix times for investigation, diagnosis and repair. Areas for improvement - A schedule of proposed changes / requests for change was to be formalised and published. There was no trend analysis of requested changes. - Testing was performed on the live system. There was no test environment to enable new functionality to be tested. Testing was limited in scope, with limited regression testing. - Going forward the Police IT Service were updating their IT service desk documentation to include M365 and the SLA within the service catalogue. - Meetings with the Azure account manager were to be scheduled and confirmed. - The M365 licence was due for renewal 1st April 2023.

1.4 Recommendation Summary

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

Critical	High	Medium	Low	Total
0	3	3	0	6

2 Engagement Objectives and Scope (Terms of Reference)

2.1 Objective

The overall objective of the review was to provide an assessment of the effectiveness of the control framework being exercised by management over the Office 365 implementation, systems, data flows and associated external processes and highlight improvements where appropriate. The review was conducted with reference to cyber security guidelines and good practice as provided by the National Cyber Security Centre (NCSC), Center for Internet Security (CIS) Microsoft 365 Foundation Benchmark v1.2.0 standards for secure email standard and cyber essentials.

2.2 Scope

The review focused upon the following areas:

- The Fire Service system, which is moving from an initial pilot to managed level of maturity.

The assessment of controls relating to the process is that at February 2023.

2.3 Approach

The following approach was adopted to enable us to evaluate potential risks, issues with controls and recommend improvements:

- We fully recognised that a number of staff were working flexibly, as such, we worked with you to agree our information requirements in advance, including at key points during the audit. This included the timetable for delivery and availability of key contacts.
- We confirmed the designated contact point at your organisation, to support the provision of the identified information requirements and to assist the audit process as required. This included providing access to the organisations systems, including the intranet, if required.
- We used software such as Skype/ MS Teams to conduct virtual meetings and to share screens to support the auditor in documenting and assessing the controls and operating effectiveness of the system being reviewed.
- Whilst working remotely, we ensured that regular contact is maintained throughout the audit process to feedback on progress and matters arising.
- We were aware that there may be restrictions which could potentially impact on the delivery of the review. We ensured that any potential issues are escalated appropriately.

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.

Technical controls and Resilience and recovery arrangements including security incident reporting	Risk Rating: High
Control design/ Operating effectiveness	
Key Finding – The tenant was implemented in line with the National Enabling Programmes (NEP) Design blueprint, however, there were weaknesses in the control design and operating effectiveness through exceptions, omissions, anomalies and work in progress. Also, business continuity plans were not yet formalised and tested. Therefore the following areas for improvement include:- • Not all the endpoint devices were compliant with the baseline, for instance supporting a Trusted Platform module (TPM) for security related functions. Bit Locker was to be implemented across all the estate. • There were instances of older versions of spreadsheets such as those used by duty managers for reporting operating on the estate. These should be upgraded, and the security configurations re-enabled to prevent these spreadsheets from operating going forward. • Users were using virtual machine “pools” for Fire / Police services. We were advised that 4 solutions were currently under investigation as they were not operating as expected in M365, such as an MS query tool (running on legacy servers) and a web development framework. 4 people using non M365 virtual machines would be impacted if access to these services was removed. Additional work was needed to ensure Fire Services operated as expected on M365. • The Fire Service were responsible for managing MS Teams accounts. A review of the MS Teams areas was to be scheduled and any excessive permissions / areas to be removed to strengthen the resilience of the estate. • There was one instance of a standalone Windows 7 desktop operating on the estate, running a legacy Human Resources database. To enable the solution to work with M365 we were advised data was to be migrated and the instance archived. • The shared home drive estate was to be migrated to OneDrive, in April 2023, with dates for personal folders to become read-only to be confirmed / implemented. • Business continuity plans were not documented, approved, and published.	
Specific Risks – Without robust arrangements in place, there is a risk that data may be managed inappropriately which could lead to loss of confidential data, potential breaches of GDPR and as a consequent financial and / or reputational damage. Arrangements may not be formalised, timely, available and / or appropriate negatively impacting services, staff and / or reputational damage.	

Security incidents may not be reported and managed in a timely fashion, putting the service at risk.

Recommendation –

1. Upgrade the estate to support TPM and enable Bit Locker encryption.
2. Migrate the older versions of spreadsheets to the latest version and prevent the older spreadsheets from operating on the estate.
3. Resolve the use of virtual machine “pools” to run M365 functionality for specific Fire Service personnel.
4. Schedule and implement a review of the MS Teams areas was to remove any excessive permissions / areas.
5. Resolve the Human Resources database and enable it to operate with M365.
6. Migrate the shared home drive estate and set a date for personal folders to become read-only.
7. Document, approve and publish business continuity plans and test.

Management Response –

No.	Commentary	Owner	Date
1	BitLocker has been in place for CFRS devices for some time. All laptops and desktops have BitLocker encryption.	Joint IT	Done
2	This recommendation pertains to 3 reports in Gartan that were produced on older versions of Excel. Gartan have updated all 3 of the reports to enable them to work in Excel 365. Security elements that were removed to enable older excel files to be opened will be reinstated to the system.	Joint IT	July-23
3	The aspiration is that all joint corporate service VM users will use Azure virtual desktops (AVD) moving forward. This will replace the current Horizon VM solution. Costs for the AVD solution have been provided but are yet to be signed off by the Service.	Joint IT/SLT	Dec-23
4	The backdoors to create Team sites found during the Teams lite implementation have been closed.	Joint IT	Done
5	All the data from the PPWIn (legacy HR) database has been migrated to an SQL database which has mitigated the concerns over loss of this data. Next steps are to build some SQL queries to assist with interrogation of the data.	HR/Payroll	Dec-23

6	The H drive will be made read only for all staff following the shift of the joint corporate service team members to the AVD. Following this access to the H drive will be revoked. Time will be provided to allow users to migrate their content to their OneDrive if they so wish.	Joint IT	Dec-23
7	The Service will work with the Joint IT team to update the relevant business continuity plans to ensure the service has a plan of action if Microsoft Services were to go down for any period of time. This will document the impacts to the Service of this downtime.	Joint IT	Mar-24

Strategy for information protection and security management | Risk Rating: High

Control design/ Operating effectiveness

Key Finding – The organisation had not set a clear data strategy to ensure appropriate usage, control, and management of the M365 applications and data. Plans to enforce stricter email access and authentication, deploy a virtual desktop and enable data management solutions were underway however, the functionality was not yet available. Also, controls were not subject to ongoing compliance and monitoring. Therefore the following areas for improvement were identified:-

- A strategy for managing data retention / cleansing data was not agreed and published although data stored on MS Teams could be requested for a relevant Freedom of information (FOI) or Subject Access Request (SAR). For instance, data had not been classified in line with an archiving, data cleansing and retention policy nor folders cleansed prior to the migration having begun. Also, we were advised that retention times for chats would be 6 months and 4 months for recordings. This was not formalised and approved.
- The Fire Service allowed email access on any device for any user. Although data policies had been configured, these were not currently enabled / enforced. For instance, emails were currently accessible from personal devices, users can copy web mails to their desktop and send personal emails to shared folders. The Fire Service allowed email access on any device for any user. Conditional access preventing access to M365 via phones unless they met a certain threshold of security when outside the service network were not yet enabled. Azure virtual desktop was to be implemented to enable stricter security controls to be enforced for accessing work email via personal devices. This was not currently deployed. InTune functionality was to be implemented across the estate. Security configurations should be enabled and the system subject to a regular assurance regime.
- We were also advised that Multi Factor / Two Factor Authentication (MFA / 2FA) were currently “light touch”. Accounts were not subject to ongoing compliance checking. The Fire

Service should also monitor login attempts that fail the second step of Multi Factor Authentication.

- Azure Information Protection, as part of the Microsoft Purview solution had not been enabled for the Fire Service instance. It aids clients to discover, classify, protect, and govern sensitive information where it resides or travels. Discussions were ongoing however, currently it was not a requirement of the Fire Service.
- A solution for searching mailboxes in support of investigations was currently not available.
- User cannot share documents using Teams Lite chat function so an alternative strategy should be agreed and published.
- Phishing exercises provided by the IT Police Service were not a requirement of the Fire Service. Training of staff about the increased threats of phishing emails, such as through regular phishing exercises / campaigns were not scheduled and assigned as part of an assurance regime.

Specific Risks - Without the appropriate data security arrangements there is a potential that data may not be fully secure. The potential risk is that vulnerabilities and gaps in controls could be exploited.

Failure to put in place robust plans and arrangements may lead to a sub-optimal and insecure deployment resulting in operational disruption, increased security incidents, loss of confidential data, potential breaches of GDPR and consequent financial and / or reputational damage.

Recommendation –

1. Document and implement a data retention, cleansing and archiving strategy, and schedule, and align it to national guidance (of 6 years to retain and then archive data).
2. Enable the technical controls for mobile phones to secure work emails via InTune. Enable security configurations for email including 2FA/MFA and schedule regular assurance regimes.
3. Monitor for login attempts that fail the second step of MFA / brute forcing of account passwords.
4. Confirm the requirements for Azure Information Protection as part of Microsoft Purview and enable, as required.
5. Confirm the solution for searching mailboxes in support of investigations.
6. Confirm the document sharing strategy for Teams Lite.
7. Schedule and perform regular phishing exercises / campaigns.

Management Response –

No.	Commentary	Owner	Date
1	CFRS have a retention schedule and have formally approved the retention timeframes for chats and recordings in Teams. This schedule will be reviewed along with national guidance in relation to cleansing and archiving data to ensure it cover all the necessary elements.	Information Management	March 2024
2	All the Services phones are now on Intune and 2FA/MFA is required when users login into their Microsoft accounts. The conditional access permissions in place will ensure the system remains secure and will negate the need for regular assurance tests.	Joint IT	Done
3	Alerts are already in place for risky sign-ins and these are sent to the security Mailbox. The Microsoft Security centre is used to monitor these by Joint IT services.	Joint IT	Done
4	Consideration will be given to the use of AIP within M365 by the Service	SIRO	Mar-24
5	Source one is currently used CFRS to search mailboxes. Consideration will be given the use Microsoft Purview/E-discovery to replace Source one once the Information management department disaggregation is completed.	Information Management	Mar-24
6	Document sharing guidance will be produced in more detail when/if the service implements the full version of Teams. Currently the service is unable to share documents with external users through Teams Lite.	TBC	Dec-23
7	Meta compliance is currently being configured and will be rolled out to CFRS staff during July.	Stuart Rogers	Jul-23

Information Governance, Risk Management, Roles, and Responsibilities	Risk Rating: High

Control design/ Operating effectiveness

Key Finding – Overarching project group and governance, and risk management including policies and a Data Privacy Impact Assessment (DPIA) were a work in progress and would have considered these controls. Therefore the following areas for improvement are highlighted:-

- There was no group overseeing the project, and would have considered the controls. We were advised that a risk management group was due to recommence at the end of January 2023 and a Member Project Board had been meeting sporadically. The organisation should reinstate appropriate group(s) to oversee the project.
- Policies to underpin system requirements for data retention, archiving and destruction, authentication / passwords, user access and controls, Bring Your Own Device (if applicable), IT security, incident management, risk management, data protection / data marking, compliance monitoring and assurance reporting for third party / supplier arrangements, etc were to be approved and published. They were not subject to compliance monitoring and assurance reporting.
- An Acceptable Use Policy (AUP) was due for review and approval in March 2022.
- We were advised that a Teams Lite Data Privacy Impact Assessment (DPIA) was in draft. Further work was needed around the requirements for managing data at rest / in transit. A clear data strategy should be produced as part of a DPIA to ensure appropriate usage, control, and management of the M365 applications and data. For instance, it should include the rules of engagement for engaging with other third parties outside the Fire Service.
- Ownership for the asset (M365) should be clearly defined. An Information Asset Owner (IAO) and project manager for the Fire Service to oversee and manage the business-as-usual activities were to be confirmed. Also, roles and responsibilities for managing the operational data and management of the M365 solution and Net Motion solution were to be confirmed.
- The Fire Service were moving Android devices, with one device currently an exception. As part of ongoing the enrolment with InTune devices should be reviewed, assets baselined and profiled, and access should only be enabled for active devices assigned an owner and line manager.
- An assurance regime, including penetration test date was not scheduled and approved.

Specific Risks – Governance and risk management arrangements do not provide for a framework which assures the Fire Service, in a routine and timely manner.

When the project is handed over from the project team to the operational teams, staff may not understand their role and responsibilities / be appropriately trained which may result in uncontrolled and inconsistent practice being observed and / or gaps or omissions

Recommendation –

1. Agree on project governance arrangements and re-instate the appropriate group(s) to oversee the project.

2. Review, approve and publish the technical / configuration policies that underpin the system requirements.
3. Review and approve the Acceptable Use Policy.
4. Document the requirements for managing data at rest / in transit as part of the Data Privacy Impact Assessment (DPIA). Formalise and approve the DPIA.
5. Confirm the IAO and project manager for the next phase of the project.
6. Confirm roles and responsibilities for managing data, M365 solution and Net Motion.
7. Confirm assets are being managed / baselined through InTune.
8. Formalise, agree and implement an assurance regime, that includes regular penetration testing.

Management Response –

No.	Commentary	Owner	Date
1	Project governance arrangements are in place through Performance and Programme board and the Senior Leadership Team where required.	Project Team	Done
2	The policies are complete and approved. They will be published in bite-sized chunks in the coming months.	SIRO	Dec-23
3	The Acceptable Use Policy has been written and is approved. See also 2, above.	SIRO	Dec-23
4	The Teams Lite DPIA was signed off and completed shortly after the audit. To be reviewed as part of the Teams implementation project	Information Management	Mar-24
5	CFRS to determine the most appropriate senior team member to become the IAO for M365.	SIRO	Dec-23
6	IT are managing the preparation of service support information for M365 to ensure it can support users who have technical issues with the M365 solution. This includes the Technical Support Manual and Service Level Agreement; it will not however cover the management of data. Management of data will be reviewed by the service in due course	Joint IT	Aug-23
7	All assets are now on Intune	Joint IT	Done

8	Penetration testing was completed in January and this looked at 365 configurations. It will be repeated each year. A screen share session can be held for evidence if required.	Joint IT	Done

Use cases for the Office 365 application	Risk Rating: Medium

Control design/ Operating effectiveness

Key Finding – The Fire Service indicated that it intended to commission Valto Microsoft IT Services to run a series of workshops to formalise the strategy / roadmaps and use cases going forward. However, analysis of departments and best deployment use case scenarios were not formalised and agreed. In particular, no use case modelling was available for the following scenarios and as a result gaps in controls were identified within this report:-

- Maintenance and management of data, such as a data retention schedule, cleansing, archiving and labelling / classification were not modelled and agreed.
- Electronic-discovery (E-discovery) was not modelled. For instance, Azure Information Protection, part of the Microsoft Purview Information Protection data protection solution was not part of its Information Governance (IG) Service provision.
- Managing user access including guest and partner organisations, dormancy, etc.
- The project team had identified 100 of the 500 mailboxes as shared mailboxes. Scope creep occurred with new use cases not officially in scope / costs not originally signed off identified during the project pilot, such as the requirement to address shared mail folders.
- Management of mailboxes and their data such as legacy and shared mailboxes
- Calendar sharing was not modelled and conformed. It will be important to move / migrate groups of users in departments together to minimise issues with access to shared mailboxes and calendars.
- Setting up a team and channels were not modelled and published.
- Use of SharePoint which was now being trialled but not modelled.
- Skype was due to be removed with the chat function for MS Teams to be used going forward. Virtual meeting solutions such as Zoom, and Webex were due to be reviewed and their roadmaps confirmed post MS Teams deployment.
- There was no use case for mobile phones. During the rollout it was discovered that MS Teams used more data than previous mobile data scenarios, with users using data rather than Wi-Fi by default, and this resulted in increased data usage costs. Going forward data usage should be modelled as part of the use case scenarios.
- Managing and maintaining assets through InTune.
- Exception cases for InTune, M365, and applications such as planner and forms, and Sway functionality (for the training team) had not been formalised and agreed.

- Users were using virtual machine “pools” for Fire / Police services. Additional work will be needed to ensure that the Fire solution requirements are fully understood for M365.

Specific Risk – Clear and agreed use cases for proposed / actual uses cases are not in place.

Recommendation –

1. Create an action plan that includes modelling, confirming, and publishing guidance for the following use cases:-
    a. Data management including defining data classification / labelling, retention, cleansing and archiving policy.
    b. Microsoft Purview to support data investigation and E-discovery.
    c. Managing access, including guests, dormancy, partner organisations, etc.
    d. Legacy / shared mailboxes and calendars.
    e. SharePoint.
    f. The chat function replacing Skype.
    g. Zoom and Webex roadmaps.
    h. Mobile phone scenarios including appropriate configuration / user guidance for data usage.
    i. Management and maintenance of assets / asset baselines through InTune.
    j. Exception cases such as applications such as planner and forms, and Sway functionality (for the training team).
    k. Solutions currently using shared services, i.e., the web development framework and MS query tool rather than running natively on M365.
    l. Future use case scenarios.
2. Continue to document decisions and schedule regular review of the action log.

Management Response –

No.	Commentary	Owner	Date
1A	The new Information Management Team within CFRS will play a key part in reviewing data management strategy and policy moving forward.	Information Management	Mar-24
1B	The Teams implementation project plans to review how Microsoft purview can be used and whether E-discovery can deliver what is required	Information Management	Mar-24
1C	Management of guest and partner accounts will be reviewed as part of the Teams implementation project. Guests and partners are not currently allowed access to CFRS M365 systems. Dormant accounts are closed after 3-6 months.	Joint IT	Done

1D	All required shared mailboxes and calendars required have been moved to M365. Mailboxes and calendars no longer required will be kept available for a period of time to be determined and then disposed of.	Joint IT	Done
1E	SharePoint will be reviewed as part of the Teams implementation project. CFRS currently only has 2 SharePoint sites - corporate docs and a legacy Blue light collaboration site which is now redundant. Use of SharePoint 365 will need to be considered for Corporate documents to ensure it remains current.	Teams Project Team	Mar-24
1F	Already completed. Awaiting Skype access to be revoked	Joint IT	Dec-23
1G	Zoom and WebEx will no longer be used by CFRS to conduct meetings as all users have Teams	Joint IT	Done
1H	All mobile phones are now upgraded to Intune and M365	Joint IT	Done
1I	All mobile phones are now upgraded to Intune and M365	Joint IT	Done
1J	Planner and Forms are already available for CFRS staff. Sway can be requested if required. When access to new M365 applications is requested a DPIA is required to be completed to ensure the risks are full understood.	Joint IT	Done
1K	The MS query issue was resolved. The plan is for all VM Horizon users to move to AVD	Joint IT	Dec-23
1L	Moving forward the Service will consider extra resource with M365 knowledge so it can better understand how it can drive further value from the M365 applications.	SLT	TBC
2	A RAID log is used daily/weekly to follow up on issues/actions as well as being used to review risks.	Project Team	Done

Up to date plans, policies, and procedures | Risk Rating: Medium

Control design/ Operating effectiveness

Key Finding – There are opportunities to improve the project planning to ensure that organisational expectations are being met and appropriate training material being produced. The following areas for improvement were identified:-

- Off-boarding the pilot project to business-as-usual was not a formally agreed phase of the project plan. Also, the Project Initiation Document (PID) did not define end dates for the pilot and off boarding the project to an operational phase of the project.
- A technical road map for future functionality / maintaining current controls was to be documented and the associated risks / issues for the next phase required a refresh technical roadmap was to be confirmed. For instance, showing the maintenance schedule for the software and hardware. It was noted that Windows 12 servers (support is due to end Oct 2023) and a Windows 10 update required factoring into future plans. Also, planned dates for example for exchange to go fully online, migration of all mailboxes to complete, webmail to migrate to the portal and enable access to be restricted, for compliance checking to be rolled out, InTune to be deployed and Airwatch archived, and for the rollout dashboards were to be confirmed. Any residual risks should be documented on the risk register.
- Further guidance / training was planned to enhance the intranet documentation. For instance, guidance to be added about how to set up public / private channels, and clearly define how long to retain recordings that involve another service or business.

Specific Risk - Clear, agreed, up-to date and monitored, plans / policies for delivery, maintenance, and compliance are not in place leading to lack of understanding regarding organisational expectations and / or potential gaps in controls that increase the potential for incidents and non-compliance to occur.

Recommendation –

1. Agree a date to transition to the operational phase of the project and formalise / approve a plan taking account of key milestones such as the rollout of dashboards and migration of functionality.
2. Document processes, for instance for managing MS Teams channels, managing access, recordings and providing guidance on how to manage recurring invitations, forwarding of invitations, and forwarding of recordings.

Management Response –

No.	Commentary	Owner	Date
1	The project is nearing completion and the project closedown and handover will be worked through in the coming months	Project Team/Joint IT	Dec-23

2	There is already a range of guidance material available on the Intranet regarding usage of Teams Lite. Further documentation will be produced as part of the Team Implementation project.	Project Team for Teams	Mar-24

Change control and support arrangements

Risk Rating: Medium

Control design/ Operating effectiveness

Key Finding – The following opportunities to strengthen the change control and support arrangements were identified:-

- A schedule of proposed changes / requests for change was to be formalised and published. There was no trend analysis of requested changes.
- Testing was performed on the live system. There was no test environment to enable new functionality to be tested. Testing was limited in scope, with testing focussed upon testing functionality had been configured as expected and limited regression testing.
- The Police IT Service were updating their service desk documentation to include M365, such as the email technical support manual. Service Level Agreements for the project were also to be formalised within the service catalogue.
- Meetings with the Azure account manager were to be scheduled and confirmed.
- The M365 licence was due for renewal 1st April 2023. This should be renewed as planned.

Specific Risks - Without appropriate change control arrangements being in place there is an increased risk of disruption that could impact service delivery and the reputation of the organisation should an event occur.

Ongoing assurance and support whilst operational may not be timely, available and / or appropriate and / or may not be compliant with legal and regulatory requirements.

Recommendation –

1. Publish a list of changes for the operational phase.
2. Formalise and agree a testing strategy.
3. Include M365 as part of the IT service documentation and the SLAs as part of the service catalogue.
4. Schedule regular meetings with the Azure account manager.
5. Renew the M365 licence .

Management Response –

No.	Commentary	Owner	Date
1	The Joint IT team produce weekly updates of changes – and can provide a forward schedule of changes. Monthly dashboards of changes that have been implemented/approved are also share with CFRS showing change trend analysis.	Joint IT	Done
2	There is no test environment available so testing will occur on the live system. Efforts are of course made to limit any impacts of Testing that occurs via use of test accounts and limited pilots. A testing strategy will be produced in conjunction with the Joint IT Team	Project Team/Joint IT	Jul-23
3	SLAs for M365 have already been produced by the Joint IT team and these are currently under-going review via a working group. As part of the project handover to BAU these will be reviewed to ensure they encompass all elements/functionality of M365	Joint IT	Oct-23
4	IT meet monthly with Microsoft. CFRS to be invited to attend future meetings	Joint IT	Done
5	Renewed in April	Joint IT	Done

Follow-up

A follow-up exercise will be undertaken during 2023-24 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.