SCOTTISH POLICE AUTHORITY

Agenda Item 3d

Meeting	**Audit, Risk and Assurance Committee**
Date	**5 May 2021**
Location	**By video conference**
Title of Paper	**Home Working Security**
Presented By	**Gary Devlin, Partner, Azets**
Recommendation to Members	**For Discussion**
Appendix Attached	**Internal Audit Report – Home Working Security**

PURPOSE

This paper presents our final report on the review of Home Working Security

The paper is presented for the Audit, Risk and Assurance Committee to consider the report, findings and management responses.

The paper is submitted for discussion.

1. BACKGROUND

1.1 Scottish Government guidance issued in response to the COVID-19 pandemic states that those who are able to work from home should do so. As a consequence, many organisations have been required to rapidly devise and implement home working arrangements.

1.2 The SPA and Police Scotland activated business continuity plans at the onset of the pandemic, which included identifying those roles that could be carried out from home with appropriate support and equipment. Over a thousand staff across the organisation were issued with equipment and transitioned to remote working across the first few weeks of the COVID-19 lockdown.

1.3 At the request of the Audit, Risk, and Assurance Committee, we have performed a review of Home Working Security. This included the arrangements for securing remote access to Police Scotland and SPA (including Forensics) IT systems, revisions to payment processes to accommodate home working, and the security of hard copy files which would normally be retained on Police Scotland, SPA, and Forensic Service premises.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Prior to the COVID-19 pandemic SPA, Police Scotland, and the Forensic Service had in place information security policies and processes that were generally robust. These have remained largely fit for purpose in a remote working context without significant modification. We have gained assurance that appropriate steps were taken to identify, assess and, where necessary, address any additional risk arising from an increased proportion of the workforce transitioned to remote working. We have identified a small number of opportunities to strengthen those controls.

3. FINANCIAL IMPLICATIONS

3.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

4. PERSONNEL IMPLICATIONS

4.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

5. LEGAL IMPLICATIONS

5.1 The Internal Audit Report considers a number of areas where the Police Service of Scotland is required to comply with legislative requirements in relation to Data Protection and the conduct of criminal proceedings. Committee members should consider this section when considering the overall implications of our findings.

6. REPUTATIONAL IMPLICATIONS

6.1 The security of information held by SPA and Police Scotland is fundamental to its organisational reputation. Committee members should consider this section when considering the overall implications of our findings.

7. SOCIAL IMPLICATIONS

7.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

8. COMMUNITY IMPACT

8.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

9. EQUALITIES IMPLICATIONS

9.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

10. ENVIRONMENT IMPLICATIONS

10.1 The Internal Audit Report considers the impact our review findings may have on organisational risk registers. Committee members should consider this section when considering the overall implications of our findings.

RECOMMENDATIONS

Members are requested to discuss the report.

Scottish Police Authority

Internal Audit Report 2020/21

Home Working Security

March 2021

Scottish Police Authority

Internal Audit Report 2020/21

Home Working Security

Audit Sponsor	***Key Contacts***	***Audit team***
Lynn Brown, SPA Chief Executive *David Page, PS Deputy Chief Officer* *Tom Nelson, Director of Forensic Services*	*Andrew Hendry, PS Chief Digital and Information Officer* *Denis Hamill, Chief Data Officer* *James Gray, Chief Financial Officer* *Jackie Dunbar, Head of Information Management* *Alice Stewart, Information Manager* *Ron Stephen, Information Security Manager* *Paul Colley, Financial Transactions Lead* *Jennifer Muir, Head of Business Support (Forensics)* *Lindsey Davie, SPA Information Management Lead*	*Gary Devlin, Audit Partner* *Paul Kelly, IT Audit Director* *Matt Swann, Internal Audit Associate Director* *Andrew Diffin, Internal Audit Assistant Manager* *Rachel Wilson, Cyber & Privacy Assistant Manager* *Will Lyburn, Senior Internal Auditor* *Carys Ross, Internal Auditor*

Executive Summary

Conclusion

Prior to the COVID-19 pandemic SPA, Police Scotland, and the Forensic Service had in place information security policies and processes that were generally robust. These have remained largely fit for purpose in a remote working context without significant modification. We have gained assurance that appropriate steps were taken to identify, assess and, where necessary, address any additional risk arising from an increased proportion of the workforce transitioned to remote working. We have identified a small number of opportunities to strengthen those controls.

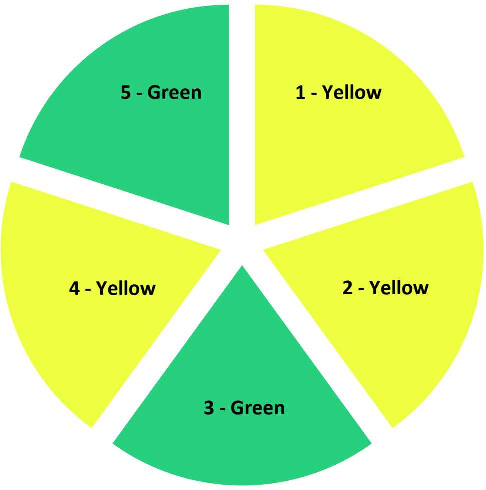
Background and scope

Scottish Government guidance issued in response to the COVID-19 pandemic states that those who are able to work from home should do so. As a consequence, many organisations have been required to rapidly devise and implement home working arrangements.

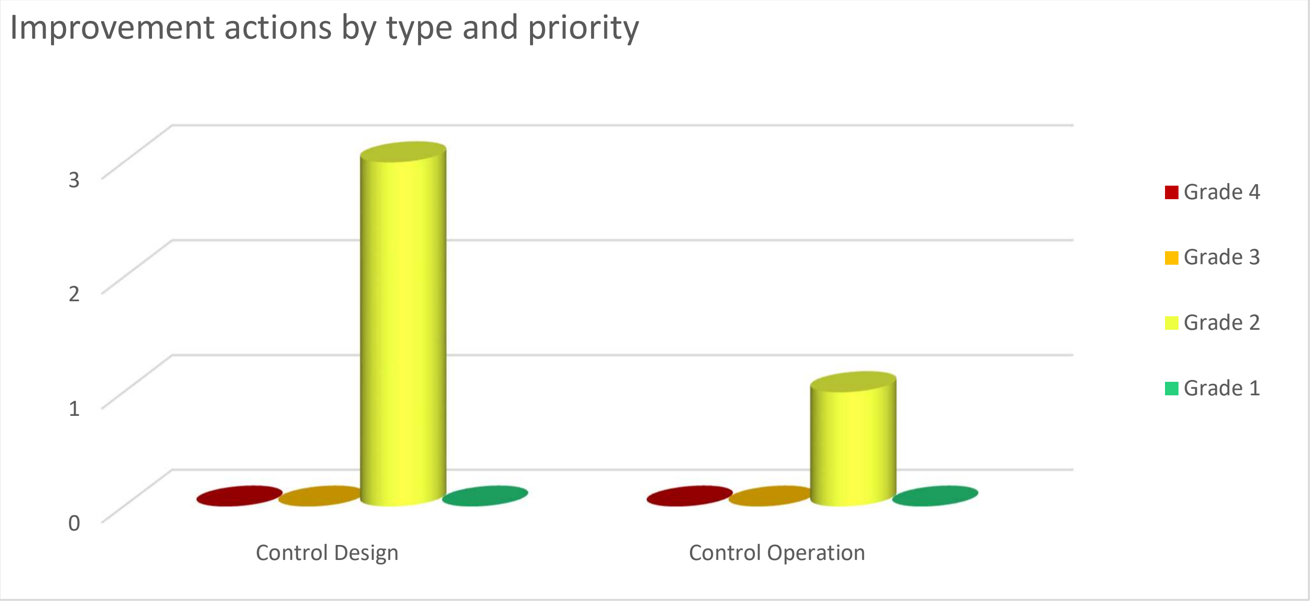
The SPA and Police Scotland activated business continuity plans at the onset of the pandemic, which included identifying those roles that could be carried out from home with appropriate support and equipment. Over a thousand staff across the organisation were issued with equipment and transitioned to remote working across the first few weeks of the COVID-19 lockdown.

At the request of the Audit, Risk, and Assurance Committee, we have performed a review of Home Working Security. This included the arrangements for securing remote access to Police Scotland and SPA (including Forensics) IT systems, revisions to payment processes to accommodate home working, and the security of hard copy files which would normally be retained on Police Scotland, SPA, and Forensic Service premises.

Control assessment



- 🟨 1. SPA and Police Scotland staff have been provided with adequate guidance and support to manage the information security risk associated with control, storage and disposal of hard copy files at home
- 🟨 2. Adequate technical solutions have been implemented to support secure remote access to the network
- 🟩 3. Access policies for purchasing systems have been updated to reflect home working arrangements
- 🟨 4. Processes for purchase authorisation, receipting, and payment are fit for purpose in the context of remote working
- 🟩 5. Security breaches are monitored and reported with action taken to address identified security issues



Four improvement actions have been identified from this review, three of which relate to the design of controls. See Appendix A for definitions of colour coding.

Key findings

Good practice

We have gained assurance that SPA, Police Scotland, and the Forensic Service's procedures reflect good practice in a number of areas:

- Police Scotland management's stated policy is that remote working should not require the removal of hard copy information from police premises. Authorisation to do so is by exception, according to a process controlled by the Information Security function.

- SPA has a clear policy, supported by guidance, which is linked to the Government Security Classification scheme and sets out the requirements for removing documentation from SPA premises and their security. These arrangements encompass the Forensic Service, and are supplemented by an established process to track the removal and return of case files from laboratories.

- Updated policies on working from home were introduced across SPA, Police Scotland, and the Forensic Service at the outset of the pandemic. This included consideration of security issues and was supported by guidance material.

- Purchasing systems have been configured such that access controls are encapsulated within the network level access controls, and these controls remained fit for purpose in a remote working context.

- There are adequate processes in place for the identification and reporting of security incidents, supported by electronic monitoring systems. Where incidents are identified, they are reviewed, triaged, and action taken.

Areas for improvement

We have a identified a number of low risk areas for improvement which, if implemented, would strengthen SPA and Police Scotland's control frameworks. These include

- Updating guidance issued to Police Scotland staff, to clarify the policy on removal of hard copy information from police premises and more clearly signpost to the relevant authorisation process.

- Ensuring that risk assessments are completed for all SPA and Police Scotland staff that have transitioned to working remotely, and that these are periodically reviewed and updated.

- Considering extending Mobile Device Management to include corporate laptops as well as mobile devices, in addition to existing encryption safeguards.

- Identifying digital equivalents to paper based process elements such as paper filing or wet signatures, and where required updating or supplementing existing process or guidance documentation such that these are applied consistently.

These points are further discussed in the management action plan below.

Impact on risk register

The SPA Corporate risk register (dated January 2021), and the Police Scotland Organisational Risk Register (dated February 2021) included the following risks relevant to this review:

- SPA Corp 017 Coronavirus – Corporate Delivery (Score 5)
- SPA Corp 019 Cyber Security (Score 5)
- PS ORR013 Information Security (Score 20)
- PS ORR116 User Access Management (Score 16)
- PS ORR071 Availability of Information held in Hard Copy (Score 16)

We have considered these risks in the context of remote working and have not identified any significant issues which suggest that the wider adoption of remote working exposes the organisation to additional, unmitigated risk. We note that the scoring of the Organisational Risks above in part reflects broader infrastructural issues in addition to any potential risk exposure arising from remote working.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Management Action Plan

Control Objective 1: SPA and Police Scotland staff have been provided with adequate guidance and support to manage the information security risk associated with control, storage and disposal of hard copy files at home.

Yellow

1.1 Police Scotland - Hard Copy Information Policy

A temporary home working policy was enacted at the onset of the pandemic setting out the responsibilities of Police Scotland staff regarding remote access, home office set ups, and the control of soft and hard copy data. This includes: requiring hard copy data to be protected when not in use and stored in a locked drawer; and prohibits the destruction of hard copy files using home shredding equipment. Guidance is available to staff on the intranet which reinforces this policy. The Information Security Handbook Divisional Guidance within the SOP sets out the formal requirements of security guidance, including GDPR compliance, for home working and is readily available to all staff on the intranet.

Throughout our review, the consistent position of Police Scotland management was that there are no circumstances where staff would be required to or would be authorised to remove hard copy files from Police premises for the purposes of remote working. A specific procedure to request authorisation from Information Management must be followed if this is required, and we understand that no such requests have been submitted. However, the Work from Home Safely Guidance and the Information Security SOP indicates that hard copy data can be stored at home if it has been authorised by line management and is stored with the appropriate security. While 'paper assets' referred to in the policy may refer to documentation created by staff such as notepads, this distinction is not clear.

Risk

There is a risk that working from home guidance for Police Scotland staff is insufficiently clear in relation to hard copy information, as it does not clearly state that specific authorisation is required from Information Management before documentation is removed from Police premises. This could limit the ability of Police Scotland to track all hard copy information removed from police premises and could lead to information (potentially sensitive) being held away from police premises without appropriate authorisation.

Recommendation

In practice, the policy applied for Police Scotland staff is that records are not permitted to be removed from Police premises. Home working guidance should be updated to clearly state this, and should signpost to the process for requesting authorisation from Information Management should a requirement to do so arise.

The guidance should also make clear that both formal records, and incidental or temporary records such as personal notepads and meeting notes, are subject to the requirements of the Information Security policy.

Grade 2 (Design)

Management Action

Management accepts this recommendation. The Interim Homeworking Guidance will be updated to address the request procedure to remove records temporarily and re-emphasis that all manual records are subject to the IS SOP/Handbook and once done ask that the notification goes out in the Line Manager's update.

Action owner: Chief Data Officer

Due date: 31 May 2021

1.2 Working From Home Risk Assessments

At the onset of the pandemic, as part of Operation Talla, business areas across SPA, Police Scotland, and the Forensic Service were required to complete an assessment to identify staff in roles suitable for remote working.

Where staff transitioned to remote working arrangements, line managers were required to complete a Home Working Risk Assessment. This requires the member of staff to confirm that they have reviewed the Home Working Guidance, Information Security SOP, and Mobile Working SOP. It includes a number of questions about the staff member's arrangements in the home to enable line managers to identify potential security concerns.

We selected a sample of 24 staff from across SPA, Police Scotland, and the Forensic Service in remote working roles and requested the risk assessment completed as part of the Operation Talla response. Of that sample of 24:

- 2 related to individuals within Police Scotland already in remote working posts and so no new assessment was completed;
- 2 assessments for Police Scotland staff could not be located (8% of our sample); and
- We received confirmation that no assessment had been completed for a further 2 members of Police Scotland staff (8% of our sample).

We did not identify any issues with the assessments carried out in relation to SPA and Forensic Services staff.

Risk

There is a risk that information security policies are not complied with, as staff transitioning to remote working have not been made aware of their requirements, resulting in the information loss or security breaches.

Recommendation

Police Scotland should ensure that Risk Assessments should be carried out for all staff transitioning to remote working. These should be stored in a central location and periodically reviewed to confirm that they remain up to date.

Management Action

Grade 2 (Operation)

Management accepts this recommendation and have/will take the following action.

1. The controls within the Operation Talla Risk Register will be updated.

2. Regular reminders have been issued to staff via the Line Manager Toolkits regarding the importance of completing Risk Assessments. We will reiterate this until a formal homeworking policy is agreed. In addition, we have used our HR Business Partners to remind Divisions of their responsibilities in this area.

Action owner: 1. Chief Data Officer **Due date:** 30 April 2021

2. Director of People & Development **Due date:** Complete

Control Objective 2: Adequate technical solutions have been implemented to support secure remote access to the network.

Yellow

2.1 Mobile Device Management

We found that a mobile device management solution is in place to track and manage the use of mobile phones issued by Police Scotland. These arrangements encompass SPA and Forensic Services devices through the IT service back arrangement between SPA and Police Scotland. The Blackberry UEM (Unified Endpoint Management) tool is used to track mobile devices, ensure that devices comply with policies such as anti-virus policies, monitor the operating software version of the device to ensure it is a supported version, and remotely wipe the device if it was lost or stolen.

We identified that laptops are not managed using a similar tool. Various controls are in place to track and monitor laptops such as the use of an asset register, and hardware encryption is used to prevent unauthorised users from accessing the content of the device if the device was lost or stolen. Staff have also been advised to securely lock away their devices in their homes when leaving the home unattended.

However, the organisation does not currently have the ability to remotely wipe a corporate laptop if it was lost or stolen. We acknowledge that IT is aware of this issue and plan to seek funding to implement a mobile device management tool which could provide this capability as part of a wider remote working business case.

Risk

There is a risk of unauthorised access to data residing on mobile devices if they were lost or stolen. This could result in personal data breaches and negative reputational impact.

Recommendation

We recommend that in order to enhance visibility of corporate assets, particularly in a remote working environment, the organisation implements a mobile device management solution which can be used to track, monitor and remotely wipe corporate laptops, if they are lost or stolen. This will also help to enhance the defence in depth model.

Management Action

Grade 2 (Design)

Management accepts the recommendation to implement a mobile device management solution which can be used to track, monitor and remotely wipe corporate laptops.

This recommendation will be actioned via the implementation of Microsoft inTune as part of the strategic implementation of the Microsoft Office 365 suite of technologies. The scope of this recommendation will be included in the design and configuration requirements for the Office 365 project to ensure it is fully actioned.

The delivery of this action via this strategic project is in the management view the most effective route and is in line with the recommendation grade (Grade 2) as opposed to a costly tactical implementation which would detract from the organisations ability to progress the strategic implementation.

The Office 365 project is on track to progress an Initial Business Case through formal governance in Q1 21/22 and is currently planning to commence implementation Q3 21/22 with the implementation being completed in Q3 22/23 subject to business case approval and funding

Action owner: Chief Technology Officer

Due date: 31 March 2023

Control Objective 3: Access policies for purchasing systems have been updated to reflect home working arrangements.

Green

No weaknesses identified

Police Scotland purchasing systems are not configured to permit direct remote access. Instead, remote access to financial systems and network drives depends upon network level access via a remote desktop solution. Accordingly, the access policies and controls specific to purchasing systems remained the same before and after the transition to remote working as these are encapsulated within general network access controls.

Each user of the Efinancials system has a unique user account and password. Requests for user accounts are administered by Finance System Analysts, and each request must be authorised by line management, and be accompanied by a Security Operating Procedures (SyOP) declaration completed by the user. The declaration signposts to Finance policies and procedures held on the Police Scotland intranet.

We reviewed Efinancials process and guidance documentation in the context of the guidance issued in relation to remote working and did not identify any inconsistency.

We selected a sample of 7 staff granted access to the Efinancials system in the last twelve months, 5 of which were processed after the commencement of Operation Talla. In all cases we were able to confirm that line manager authorisation had been recorded, and that the SyOP declaration had been completed and retained.

Control Objective 4: Processes for purchase authorisation, receipting, and payment are fit for purpose in the context of remote working.

Yellow

4.1 Purchasing Processes

The Police Scotland Finance function introduced digital document handling prior to the onset of the Covid pandemic, meaning that purchase processing was largely paperless at the point at which the organisation began to transition to remote working. Purchasing processes and guidance documentation were not updated or supplemented specifically in relation to remote working, as processes were able to operate as normal.

Guidance documentation retains references to printing documents and retaining manual signoffs, for example in guidance relating to the processing of purchase orders. We understand that these are interpreted in the context of remote working to refer to digital equivalents, however there is no consistent, documented approach.

We have not identified any specific instance in which this leads to ambiguity in the course of this review, however we note that more detailed testing has been carried out in the course of our reviews of Payroll and Non-Pay Expenditure.

Risk

There is a risk that inconsistent approaches to the retention of audit trails, as a consequence of a lack of clear guidance, creates opportunities to subvert authorisation controls. This could increase the risk of the processing of unauthorised or fraudulent payments.

Recommendation

Police Scotland should review its existing guidance to update references to manual controls, or issue supplementary guidance. In either case, a consistent approach to applying digital equivalents to manual or paper based controls should be adopted and clearly communicated.

Management Action

Grade 2 (Design)

Management accepts this recommendation. References to "printing" in the purchasing guidance are due to the naming of the functionality within eFinancials, where hitting the button "print" generates a PDF purchase order which is subsequently emailed to the supplier and never physically printed. This is well understood amongst existing users of eFinancials Purchase Order Processing module. However as noted, the organisation is in the process of moving to a wholly electronic requisitioning and approval system via the eProcurement module and fully electronic approval of non-purchase order invoices via additional functionality for e-invoicing and electronic authorisation workflow (Cloudtrade and Purchase Invoice Manager). The project team will ensure that any references to printing in the new guidance relating to those system deployments makes it clear that is equivalent to generating a PDF and manual signatures will only be required for authorisation in a business continuity event preventing access to eFinancials/PIM for a prolonged period.

Action owner: Interim Head of Procurement & Stores **Due date:** 31 May 2021

Control Objective 5: Security breaches are monitored and reported with action taken to address identified security issues.

Green

No weaknesses identified

Responsibilities in relation to the monitoring, reporting, and response to Security breaches are defined in the SPA and Police Scotland Information Security SOPs. Both SOPs include a definition of "Information Security Incident" which encompasses Data Breaches within the scope of the GDPR. All staff have a responsibility to report security breaches, and this is communicated through policy and guidance which is made available on the staff intranet and supported by training. At time of audit, Police Scotland Information Security had logged 1260 Information Security incidents for the first three quarters of 2020/21, of which only 1 was required to be reported to the ICO. The majority of these incidents (1,061 or 84%) related to email misuse. SPA Information Management had logged 1 incident relating to the Forensic Service, which was not required to be reported to the ICO.

Police Scotland and SPA Guidance both outline reporting processes and timescales, supported by template documentation. Within the Forensic Service, the quality management system Q-Pulse is used to log security breaches and subsequently report these to SPA Information Management.

Monitoring of IT infrastructure and email communication is carried out by Police Scotland Information Management through the use of Security Information and Event Management (SIEM) solution, ArcSight. Email communication is monitored by Mail Marshall, which scans and quarantines email sent to high risk addresses. We reviewed the triage queues of both systems to confirm that exceptions are actively monitored. Responses to incidents are identified and implemented according to the Information Security SOP, Data Loss Incident Process, and Cyber Incident Response plan.

Within Police Scotland, reporting is prepared on a quarterly basis and reviewed by the Data Governance Board, whose remit includes the exercise of Senior Information Risk Owner (SIRO) authority and responsibility for information risks. Onward reporting is presented to the SPA Audit and Risk Committee, and externally as required to the Home Office and Information Commissioner's Office (ICO). The SPA Information Management Lead prepares reporting in respect of SPA and the Forensic Service, which are reported to the SPA Chief Executive and Director of Forensic Services, and ultimately to the Audit and Risk Committee on a six-monthly basis. We reviewed a sample of reports to confirm that these processes are operating as expected, and reviewed action taken in response to incidents for reasonableness, with no issues identified.

Appendix A – Definitions

Control assessments

R Fundamental absence or failure of key controls.

A Control objective not achieved - controls are inadequate or ineffective.

Y Control objective achieved - no major weaknesses but scope for improvement.

G Control objective achieved - controls are adequate, effective and efficient.

Management action grades

4 •Very high risk exposure - major concerns requiring immediate senior attention that create fundamental risks within the organisation.

3 •High risk exposure - absence / failure of key controls that create significant risks within the organisation.

2 •Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risks within the organisation.

1 •Limited risk exposure - controls are working effectively, but could be strengthened to prevent the creation of minor risks or address general house-keeping issues.

Appendix B – Summary of management actions

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
1.1	**Police Scotland - Hard Copy Information Policy** In practice, the policy applied for Police Scotland staff is that records are not permitted to be removed from Police premises. Home working guidance should be updated to clearly state this, and should signpost to the process for requesting authorisation from Information Management should a requirement to do so arise. The guidance should also make clear that both formal records, and incidental or temporary records such as personal notepads and meeting notes, are subject to the requirements of the Information Security policy.	Management accepts this recommendation. The Interim Homeworking Guidance will be updated to address the request procedure to remove records temporarily and re-emphasis that all manual records are subject to the IS SOP/Handbook and once done ask that the notification goes out in the Line Manager's update.	2	Chief Data Officer	31 May 21
1.2	**Working From Home Risk Assessments** Police Scotland should ensure that Risk Assessments should be carried out for all staff transitioning to remote working. These should be stored in a central location and periodically reviewed to confirm that they remain up to date.	Management accepts this recommendation and have/will take the following action. 1. The controls within the Operation Talla Risk Register will be updated. 2. Regular reminders have been issued to staff via the Line Manager Toolkits regarding the importance of completing Risk Assessments. We will reiterate this until a formal homeworking policy is agreed. In addition, we have used our	2	1. Chief Data Officer 2. Director of People & Development	30 Apr 21 Complete

		HR Business Partners to remind Divisions of their responsibilities in this area.			
2.1	**Mobile Device Management** We recommend that in order to enhance visibility of corporate assets, particularly in a remote working environment, the organisation implements a mobile device management solution which can be used to track, monitor and remotely wipe corporate laptops, if they are lost or stolen. This will also help to enhance the defence in depth model.	Management accepts the recommendation to implement a mobile device management solution which can be used to track, monitor and remotely wipe corporate laptops. This recommendation will be actioned via the implementation of Microsoft inTune as part of the strategic implementation of the Microsoft Office 365 suite of technologies. The scope of this recommendation will be included in the design and configuration requirements for the Office 365 project to ensure it is fully actioned. The delivery of this action via this strategic project is in the management view the most effective route and is in line with the recommendation grade (Grade 2) as opposed to a costly tactical implementation which would detract from the organisations ability to progress the strategic implementation. The Office 365 project is on track to progress an Initial Business Case through formal governance in Q1 21/22 and is currently planning to commence implementation Q3 21/22 with the implementation being completed in Q3 22/23 subject to business case approval and funding	2	Chief Technology Officer	31 Mar 23

4.1	**Purchasing Processes** Police Scotland should review its existing guidance to update references to manual controls, or issue supplementary guidance. In either case, a consistent approach to applying digital equivalents to manual or paper based controls should be adopted and clearly communicated.	Management accepts this recommendation. References to "printing" in the purchasing guidance are due to the naming of the functionality within eFinancials, where hitting the button "print" generates a PDF purchase order which is subsequently emailed to the supplier and never physically printed. This is well understood amongst existing users of eFinancials Purchase Order Processing module. However as noted, the organisation is in the process of moving to a wholly electronic requisitioning and approval system via the eProcurement module and fully electronic approval of non-purchase order invoices via additional functionality for e-invoicing and electronic authorisation workflow (Cloudtrade and Purchase Invoice Manager). The project team will ensure that any references to printing in the new guidance relating to those system deployments makes it clear that is equivalent to generating a PDF and manual signatures will only be required for authorisation in a business continuity event preventing access to eFinancials/PIM for a prolonged period.	2	Interim Head of Procurement & Stores	31 May 21