SCOTTISH POLICE AUTHORITY

Meeting	**SPA Audit Committee**
Date	**20 June 2018**
Location	**Fettes Police Station, Edinburgh**
Title of Paper	**ICO Overview**
Item Number	**4**
Presented By	**Robin Johnstone, Head of Legal, SPA** ***(on behalf of SPA Director, Governance & Assurance)***
Recommendation to Members	**For Noting**
Appendix Attached	**Yes** **A – ICO Executive Summary Report** **B – ICO Report** **C – Recommendations Tracker**

PURPOSE

1. To invite the Audit Committee to consider the ICO report, its associated recommendations tracker and to note progress to date.

The paper is presented in line with Scottish Police Authority Audit Committee Terms of Reference
http://www.spa.police.uk/assets/128635/293617/376046/committeetor2018

The paper is submitted:

- **For Noting** in relation to update on progress against ICO recommendations.

1. BACKGROUND

1.1 This item was requested by Audit Committee Members, in order to have an opportunity to understand the ICO Audit on SPA. Members should note that Police Scotland were in receipt of a separate ICO Audit Report, and is not referenced in this report.

2. FURTHER DETAIL ON THE REPORT TOPIC

Timeline

2.1 The Office of the Information Commissioner (ICO) were advised of a Forensics data breach in April 2014. SPA and Police Scotland jointly agreed to report the incident to ICO.

2.2 After initial assessment of the report, ICO offered a 'consensual audit'.

2.3 The Police Scotland audit took place in summer 2016, and the SPA audit took place in summer 2017.

2.4 The audit for SPA focused on 3 areas; Training, Security and Data Sharing. The auditors visited Pacific Quay and the Crime Campus in August 2017 and interviewed a number of staff. The audit resulted in 120 recommendations being proposed in September 2017. From this initial draft, SPA Information Management Team were asked to give feedback on factual inaccuracies – not all feedback was accepted.

2.5 The final audit report in October 2017 had 117 recommendations. Of those, SPA rejects 19. There were 28 urgent recommendations, 72 high, 10 medium and 7 low.

2.6 Of the 98 recommendations that SPA accepts, all but 13 will be covered by the GDPR project.

2.7 (For noting: An example of a rejected recommendation is that 'SPA enforce password changes'. SPA does enforce password changes and always has done.)

2.8 The final ICO audit report was received by SPA Information Management on 27 February 2018.

2.9 ICO published an Executive Summary on 11 April 2018, and Board Members were advised of this by an email from SPA Corporate Communications on 13 April 2018.

Status Update

2.10 The majority of the ICO recommendations are captured by actions required to discharge the GDPR readiness action plan, a copy of which is circulated to the Chair of the Audit Committee on a fortnightly basis, and has been the subject of regular reporting to the Audit Committee.

2.11 For complete visibility, the ICO action plan with associated updates is attached to this report for awareness. This was previously circulated to the Chair of the Audit Committee at the beginning of May 2018. Work is ongoing to prepare an updated version of this document based on the impending audit of GDPR work, and can be available for the next planned meeting of the Audit Committee in July.

2.12 There is due to be an internal audit of GDPR compliance next week (w/c 25 June 2018), and the updated GDPR action list will be circulated to the Audit Committee after the Project Board meeting on Monday morning as per the normal fortnightly update.

2.13 Following the 'round up' of the initial GDPR readiness project, the management of ongoing work will be overseen by the Information Governance Forum which consists of SIRO, SPA Information Management, Forensics, Legal, HR Governance, and Police Scotland IT. This will take effect from July 2018.

2.14 SPA will be required to formally advise ICO on progress against the recommendations when they do a follow up audit, currently tentatively scheduled for August 2018.

2.16 Committee Members should be advised that the full ICO audit report and email communication were released by ICO under a recent FOI.

3. FINANCIAL IMPLICATIONS

3.1 There **are no** financial implications in this report.

4. PERSONNEL IMPLICATIONS

4.1 There **are** personnel implications associated with this paper.

4.2 The Information Management Team consist of two permanent members of staff who have a range of responsibilities including FOI's, Subject Access Requests, rolling out GDPR compliance, information security, training staff within SPA Corporate and Forensics, assessing meeting locations for security, maintaining

professional networks and relevant accreditations.

4.3 The team have recently been supplemented by a temporary resource, who will be with us until 27 January 2019. That individual will be working on ensuring the documentation and legal processing agreements are in place with all relevant external bodies.

4.4 In a wider workload context, FOI's and Subject Access Requests have significantly increased over the last 6 months. There is a balancing act of meeting statutory timescales in all these areas, implementing improvements and ensuring that the team are resilient. There have been periods of absence across the team since December 2017.

5. LEGAL IMPLICATIONS

5.1 There **may be** legal implications in this paper. Based on how effectively SPA has discharged the recommendations, any follow up audit may require additional legal advice in relation to any non-compliance issues.

6. REPUTATIONAL IMPLICATIONS

6.1 There **may be** reputational implications associated with this paper. SPA will focus on ensuring compliance with the report and seek to discharge the recommendations within reasonable timescales.

7. SOCIAL IMPLICATIONS

7.1 There **are no** social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There **are no** community implications associated with this paper.

9. EQUALITIES IMPLICATIONS

9.1 There **may be** equality implications associated with this paper. All associated actions resulting in changes to the ways in which SPA operate will require to have an EqHRIA undertaken. Those will be assessed on a case by case basis.

10. ENVIRONMENT IMPLICATIONS

10.1 There **are no** environmental implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

1. Note the information contained within this report;

2. Determine what, if any, further information is required post-meeting, not already covered through normal reporting schedules.

Scottish Police Authority

Data protection audit report

Executive summary

Information Commissioner's Office

1. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

In December 2014 the Scottish Police Authority (SPA) and Police Service of Scotland (PSoS) self-reported an information security breach which occurred in April 2014. The breach involved the loss of an unencrypted data stick containing sensitive personal data relating to 15 criminal investigations. The ICO Enforcement Department conducted an investigation and this resulted in a recommendation that a consensual audit would be the most effective way of improving compliance within SPA. The ICO recommended the following remedial action:

1. This breach highlighted the use of unencrypted devices within the organisation. Please ensure that unencrypted devices are not used for the storage and transportation of personal data, by third parties with whom personal data is shared or by the Scottish Police Authority itself.

2. Please ensure that the organisation has information sharing protocols in place between itself and other third parties where personal data is shared including Police Scotland.

3. Please ensure that staff awareness of DP issues continues to be raised by ensuring good attendance rates at any mandatory DP training the organisation may provide and that this training is regularly reviewed and updated as necessary, with refresher training being provided as appropriate. Please ensure that the organisation is able to track attendance on such training.

SPA agreed to a consensual audit by the ICO of its processing of personal data.

A teleconference was held on 25 May 2017 with representatives of SPA to identify and discuss the scope of the audit.

The audit field work was undertaken at SPA Pacific Quay and Scottish Crime Campus, Gartcosh, Glasgow between 8 and 10 August 2017.

2. Scope of the audit

Following pre-audit discussions with SPA it was agreed that the audit would focus on the following areas:

Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

Training and awareness – The provision and monitoring of staff data protection and information security training and the awareness of data protecting and information security requirements relating to their roles and responsibilities.

Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit Approach

The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

The purpose of the audit was to provide the Information Commissioner and SPA with an independent opinion of the extent to which SPA within the scope of this agreed audit, is complying with the DPA.

Where areas for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

In order to assist data controllers in implementing the recommendations each recommendation has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

It is important to note that the above ratings are assigned to the recommendations based upon the ICO's assessment of the risks involved. SPA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

4. Audit opinion

The purpose of the audit is to provide the Information Commissioner and SPA with an independent opinion of the extent to which SPA, within the scope of this agreed audit, is complying with the DPA.

Overall Conclusion	
Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment. We have made two very limited and one limited assurance assessments where controls could be enhanced to address the issues which have been identified.

5. Summary of Recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of the DPA.	We have made **28** urgent priority recommendations across all three scope areas: **17** in Information Security; **5** in Training and Awareness and **6** in Data Sharing where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **72** high priority recommendations across all three scope areas: **39** in Information Security; **18** in Training and Awareness and **15** in Data Sharing where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **10** medium priority recommendations across all three scope areas: **3** in Information Security; **6** in Training and Awareness; and **1** in Data Sharing where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **7** Low priority recommendations across two scope areas: **4** in Information Security; and **3** in Training and Awareness where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

There is an overall Information Security policy in place supported by some topic-specific related policies and procedures. This includes the Physical and Environmental Security Policy, Electronic Communications SOP and the Remote Working Policy. In addition to information security related policies and SOPs, SPA also has a Data Protection and Records Management Policy.

Desktops and remote devices have Symantec endpoint controls in place to ensure that staff cannot use unauthorised USBs.

Areas for improvement

PSoS provides SPA with ICT services. SPA does not have a written supplier agreement in place with PSoS which includes clear instructions that defines what they can or cannot do with the data accessed as part of the services.

Risk management within SPA does not include information risks. Whilst both a Risk Management Policy and corporate risk register are in place there is no inclusion of information risks.

Privacy impact assessments (PIAs) are not carried out for all new projects and changes to existing systems. PIAs are also not completed to make informed decisions about whether to proceed with information sharing.

There is no effective asset management within SPA. There is no information asset register in place which records both physical and electronic assets held. Information Assets Owners (IAO) have not been established for all assets.

SPA does not have an Access Control Policy in place which defines procedures for Line Management and HR to follow in the event of a new starter/leaver or mover. Due to the lack of communication between departments, access to systems is not effectively managed.

Physical security risk assessments are not carried out by the Information Management Team (IMT) across SPA.

There is no Incident Management Policy in place which clearly defines staff responsibilities and the requirement to report information security incidents to IMT.

There is no formal data protection or information security training programme in place for SPA.

Delivery of training is not consistent within corporate departments and Forensic Services. Whilst the Head of Information Management (HoIM) is responsible for conducting training for corporate SPA, this does not extend to Forensic Services.

SPA does not mandate any data protection or information security refresher training.

SPA regularly shares information with third parties including PSoS, the Crown

Office and Procurator Fiscal Service (COPFS) and the Police Investigations and Review Commissioner (PIRC). SPA do not have formal Data Sharing Agreements (DSAs) in place with any of these separate agencies.

SPA do not provide data subjects with fair processing information or seek consent to share information with third parties where necessary.

SPA does not have processes in place to ensure that shared data is kept accurate and up to date.

SPA does not seek assurance that shared data is deleted or securely destroyed in line with the agreed retention period.

Scottish Police Authority

Data protection audit report

Auditors:	Gurdeep Kaur – Engagement Lead Auditor Emma Bennett – Lead Auditor Charlotte Haywood – Lead Auditor Mandy Enfield – Team Manager
Data controller contacts:	Lindsey Davie – Head of Information Management Carol-Anne Hilley – Records Manager
Distribution:	Kenneth Hogg – Chief Executive Officer Lindsey Davie – Head of Information Management Carol-Anne Hilley – Records Manager
Date of first draft:	25 August 2017
Date of second draft:	25 September 2017
Date of final draft:	12 February 2018
Date issued:	**February 2018**

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Scottish Police Authority.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 In December 2014 the Scottish Police Authority (SPA) and Police Service of Scotland (PSoS) self-reported an information security breach which occurred in April 2014. (ICO case reference COM0564622). The breach involved the loss of an unencrypted data stick containing sensitive personal data relating to 15 criminal investigations. The ICO Enforcement Department conducted an investigation and this resulted in a recommendation that a consensual audit would be the most effective way of improving compliance within SPA. SPA was required to undertake the following remedial action:

1. This breach highlighted the use of unencrypted devices within the organisation. Please ensure that unencrypted devices are not used for the storage and transportation of personal data, by third parties with whom personal data is shared or by the Scottish Police Authority itself.

2. Please ensure that the organisation has information sharing protocols in place between itself and other third parties where personal data is shared including Police Scotland.

3. Please ensure that staff awareness of DP issues continues to be raised by ensuring good attendance rates at any mandatory DP training the organisation may provide and that this training is regularly reviewed and updated as necessary, with refresher training being provided as appropriate. Please ensure that the organisation is able to track attendance on such training.

1.4 SPA has agreed to a consensual audit by the ICO of its processing of personal data.

1.5 A teleconference was held on 25 May 2017 with representatives of SPA to identify and discuss the scope of the audit.

1.6 The audit field work was undertaken at SPA Pacific Quay and Scottish Crime Campus, Gartcosh, Glasgow between 8 and 10 August 2017.

2. Scope of the audit

2.1 Following pre-audit discussions with SPA it was agreed that the audit would focus on the following areas:

Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

Training and awareness – The provision and monitoring of staff data protection and information security training and the awareness of data protection and information security requirements relating to their roles and responsibilities.

Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

3. Audit Approach

3.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

3.2 The purpose of the audit was to provide the Information Commissioner and SPA with an independent assurance of the extent to which SPA within the scope of this agreed audit, is complying with the DPA.

3.4 Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

3.5 In order to assist data controllers in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact					
	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

3.6 It is important to note that the above ratings are assigned based upon the ICO's assessment of the risks involved. SPA's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

4. Audit grading

4.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Definitions
	High assurance	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the DPA.
	Reasonable assurance	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.
	Limited assurance	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.
	Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

5. Audit opinion

5.1 The purpose of the audit is to provide the Information Commissioner and SPA with an independent assurance of the extent to which SPA, within the scope of this agreed audit, is complying with the DPA.

Overall Conclusion	
Very limited assurance	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment. We have made two very limited and one limited assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 8 of this report, along with management responses.

6. Summary of Recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of the DPA.	We have made **28** urgent priority recommendations across all three scope areas: **17** in Information Security; **5** in Training and Awareness and **6** in Data Sharing where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **72** high priority recommendations across all three scope areas: **39** in Information Security; **18** in Training and Awareness and **15** in Data Sharing where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **10** medium priority recommendations across all three scope areas: **3** in Information Security; **6** in Training and Awareness; and **1** in Data Sharing where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **7** Low priority recommendations across two scope areas: **4** in Information Security; and **3** in Training and Awareness where controls could be enhanced to address the issues identified.

7. Summary of audit findings

7.1 Areas of good practice

There is an overall Information Security policy in place supported by some topic-specific related policies and procedures. This includes the Physical and Environmental Security Policy, Electronic Communications SOP and the Remote Working Policy. In addition to information security related policies and SOPs, SPA also has a Data Protection and Records Management Policy.

Desktops and remote devices have Symantec endpoint controls in place to ensure that staff cannot use unauthorised USBs.

7.2 Areas for improvement

There is a lack of oversight by SPA regarding the management and control of the ICT services provided by PSoS. SPA does not have a written supplier agreement in place with PSoS which includes clear instructions that defines what they can or cannot do with the data accessed as part of the service.

Risk management within SPA does not include information risks. Whilst both a Risk Management Policy and corporate risk register are in place there is no inclusion of information risks.

Privacy impact assessments (PIAs) are not carried out for all new projects and changes to existing systems. PIAs are also not completed to make informed decisions about whether to proceed with information sharing.

There is no effective asset management within SPA. There is no information asset register in place which records both physical and electronic assets held. Information Assets Owners (IAO) have not been established for all assets.

SPA does not have an Access Control Policy in place which defines procedures for Line Management and HR to follow in the event of a new starter/leaver or mover. Due to the lack of communication between departments, access to systems is not effectively managed.

Physical security risk assessments are not carried out by the Information Management Team (IMT) across SPA.

There is no Incident Management Policy place which clearly defines staff responsibilities and requirements to report all information security incidents to IMT.

There is no formal data protection or information security training programme in place for SPA.

Delivery of training is not consistent within corporate departments and Forensic Services. Whilst the Head of Information Management (HoIM) is responsible for conducting training for corporate SPA, this does not extend to Forensic Services.

SPA does not mandate any data protection or information security refresher training.

SPA regularly shares information with third parties including PSoS, the Crown Office and Procurator Fiscal Service (COPFS) and the Police Investigations and Review Commissioner (PIRC). SPA do not have formal Data Sharing Agreements (DSAs) in place with any of these separate agencies.

SPA do not provide data subjects with fair processing information or seek consent to share information with third parties where necessary.

SPA does not have processes in place to ensure that shared data is kept accurate and up to date.

SPA does not seek assurance that shared data is deleted or securely destroyed in line with the agreed retention period.

8. Detailed findings and action plan

8.1 Scope A: Information Security - There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

Risk: Without appropriate measures there is a risk of non-compliance with the seventh principle of the DPA. This may result in damage and/or distress for individuals who are the subject of the data, and reputational damage for the organisation as a consequence of this and any regulatory action taken by the Information Commissioner.

Recommendations	
Urgent:	17
High Priority:	39
Medium Priority:	3
Low Priority:	4

Organisation – Internal Organisation

a1. The SPA is responsible for maintaining policing and for the management of Forensic Services in Scotland. SPA is divided into corporate departments and Forensic Services. Corporate departments are based at the SPA headquarters in Pacific Quay (PQ), Glasgow.

a2. It was reported that there are approximately 500 staff employed within Forensic Services. There are approximately 200 staff located at the Scottish Crime Campus in Gartcosh, 100 staff in Dundee and the remaining deployed across Scotland between Edinburgh and Aberdeen in co-located premises.

a3. Information security responsibilities sit within the Information Management Team (IMT) in the Governance and Assurance Directorate.

a4. The Director of Governance and Assurance (DoGA) is the SPA's Senior Information Risk Owner (SIRO). However, due to long term absence, the Head of Legal and Compliance (HoLC) has recently been assigned the role of SIRO. The HoLC job description has not been updated to reflect the additional responsibilities of the SIRO role.

Priority Recommendation: Low.
Ensure the HoLC's job description is updated to reflect new role and responsibilities of acting SIRO.

Management response: Rejected.
Job descriptions are not updated for 'acting' roles

a5. The IMT consists of the HoIM and the Records Manager (RM). The HoIM reports to the HoLC. The HoIM is responsible for the development of policies and procedures, providing advice on information assurance, creating data sharing agreements (DSA) /Memorandum of Understandings (MoU), implementing a programme of risk assessments and audits and accreditation for IT systems.

a6. The RM reports directly to the HoIM and key information security responsibilities include assisting the HoIM with data protection and information security compliance and assist with security breach investigation.

a7. The Information Security Standard Operating Procedure (IS SOP) states that the Chief Executive Officer (CEO) has overall responsibility for assessing information risks. The responsibility will be supported by the SIRO who will delegate tasks to Information Assurance Officers, Technical Security Manager, Information Asset Owners (IAOs) and Accreditor. The IS SOP does not clearly outline the responsibilities of the current roles in place within the SPA e.g. HoIM, RM.

Priority Recommendation: High.
Review the current IS SOP to clearly define and outline responsibilities of key information security roles within SPA. The IS SOP should make reference to the roles and responsibilities of the SIRO, HoIM, RM and IAOs. Finding where there was an uncontrolled or poorly controlled risk that will require a recommendation to improve practices.

Management response: Accepted

Owner: HoIM
Date for implementation: End October 2017

a8. SPA's ICT services are provided by PSoS. There is a lack of oversight by SPA regarding the management and control of the ICT services provided.

Priority Recommendation: Urgent.
Where a third party (PSoS) is providing SPA with an ICT Service, the relationship and processing should be formally documented in a written contract. The supplier relationship agreement should include clear instructions to the ICT service provider defining what they can or cannot do with the data. The written contract should require the ICT service provider to act on SPA's instructions only. Please see recommendation at **a82** in the 'Supplier Relationships' section.

Management response: Accepted
SPA have sought permission to engage a specialist lawyer to manage this issue with Police Scotland. This is part of the bigger overall issue of the data controller/data processor relationship that needs to be resolved prior to GDPR.

Owner: Director Governance & Assurance
Date for implementation: May 2018

a9. The Risk and Policy Officer is responsible for risk management within SPA. There is a Risk Management Policy which outlines SPA's approach to the management of risks. This Policy does not specifically make reference to the management of information risks; the policy was last reviewed in 2015.

Priority Recommendation: High.
Review the current Risk Management Policy to ensure the policy outlines SPA's approach to information risk management. To ensure the content remains accurate and fit for purpose, ensure the policy is reviewed on annual basis.

Management response: Rejected.

a10. The Risk Management Policy is accompanied by a Risk Matrix. Risks identified within SPA are assessed and provided with a probability and impact score between one and five. Probability is multiplied by impact to get the overall risk score.

a11. There is a corporate risk register in place. The risk register records a description of the risk, mitigating plan, method of risk assessment, risk management status, risk owner and calculated risk score. Access to the corporate risk register was not provided to Auditors during the onsite visit. It was reported by the Risk and Policy Officer that information risks are not recorded on the overall corporate risk register. The HoIM reported that information risks have been previously escalated to be added to the corporate risk register however, the HoIM has no direct involvement with the register.

Priority Recommendation: Urgent.
Ensure the corporate risk register includes SPA's information risks. Alternatively, create a separate information risk register. Similar to the current corporate risk register, the register should record a description of the risk, mitigating plan, rating and risk owner. The HoIM should be consulted in relation to all information risks to ensure all risks are effectively managed and mitigated.

Management response: Accepted
Information Management risks will be included within the SPA Corporate Risk Register. Any member of staff can propose risks to be added to the corporate risk register. New risks are reported to the Senior Management Group to approve inclusion in the risk register and also reported to SPA Audit Committee for noting. The HoIM will liaise with the risk and policy specialist to highlight relevant risks, taking cognisance of the audit findings, for inclusion in the corporate risk register.

Since the audit was completed a risk has been added to the corporate risk register relating to GDPR.

Owner: Director of Strategy and Performance
Date for implementation: In place

a12. Forensic Services also maintains a local risk register, however it was reported by the Director of Forensic Services that the departmental risk register does not include information risks.

Priority Recommendation: Urgent.
Ensure the local risk register maintained by Forensic Services includes information risks. Please refer to recommendation at **a11**.

Management response: Partially Accepted

Owner: Director of Forensic Services
Date for implementation: January 2018

a13. PSoS does not maintain a local ICT risk register for SPA. It is unclear if ICT related information risk are reported and included on the SPA corporate risk register.

a14. It was reported that the top 10 risks recorded on the corporate register are reported to the Audit and Risk Committee (Committee). The Risk and Policy Officer is responsible for reporting to the Committee every quarter.

a15. The Data Protection Policy states that any new collection of data will be subject to a PIA. PIAs must be completed by project leads and provided to IMT. However, PIAs are not carried out for all new projects or significant changes to existing systems. It was reported that the HoIM has previously been consulted by the Forensic Services to carry out assessments; however, this has been after the system has been purchased.

Priority Recommendation: Urgent.
Create a PIA policy which sets out the requirement to conduct PIAs on all new projects, or changes to current processes that involve personal data to assess and identify information security risks. The PIA Policy should require project leads to conduct a PIA at the beginning of the project or change, to identify information risks and controls to mitigate those risks. Requiring a PIA to be conducted for projects and changes to existing systems will assist with the changes that are required to be implemented when GDPR is implemented in May 2018.

Management response: Accepted

Owner: HOIM
Date for implementation: November 2018

a16. As previously mentioned, there is a Committee in place for SPA to report on information security incidents and risks. Attendees of the Committee involve representatives from SPA, PSoS and external auditors Scott Moncrieff. The previous SIRO attended the Committee with the Director of Finance. At present, the acting SIRO has not yet attended a meeting.

Priority Recommendation: Medium.
To ensure there is an appropriate representative to discuss and report key information security issues to the Committee, ensure arrangements are made for the acting SIRO to attend quarterly meetings.

Management response: Accepted.

Owner: Director of Governance & Assurance
Date for implementation: Complete by 1st Quarter 2018

a17. SPA has no other steering/working groups in place to discuss and report key information security issues across both corporate and forensic services.

Priority Recommendation: High.
Introduce a regular forum or steering group to discuss and report information security issues identified across the SPA. This group should be chaired by an appropriate senior level of staff i.e. SIRO and attendance should include key roles from departments across both corporate and forensic services. Attendance should include a member of PSoS IT service delivery team to report on IT related concerns.

Management response: Accepted

Owner: Director of Governance & Assurance
Date for implementation: November 2017

a18. It was reported that a representative of SPA attends the PSoS IT working group chaired by the Director of IT. However, as the current SPA representative is not a subject matter expert, concerns were expressed that key issues, risks or other security concerns discussed/raised are not effectively reported back.

Priority Recommendation: High.
High: Identify an appropriate role to attend the PSoS IT working group to ensure SPA has oversight of key issues and concerns discussed.

Management response: Accepted

Owner: CEO
Date for implementation: Will be in place for next scheduled meeting in 2018.

Policy Management Direction

a19. There is an overarching IS SOP. The HoIM is responsible for the ownership of the IS SOP which was last reviewed in November 2016.

a20. The purpose of the IS SOP is to formalise management direction and support for the security of SPA systems. The IS SOP includes information classification and control, roles and responsibilities, accreditation and audit, codes of connection, cryptography, procurement, reporting incidents, secure disposal and access control.

a21. The IS SOP is supported by some topic-specific related policies and procedures. This includes the Physical and Environmental Security Policy, Electronic Communications SOP and the Remote Working Policy. In addition to information security related policies and SOPs, SPA also has a Data Protection and Records Management Policy.

a22. All corporate SPA policies and SOPs reviewed included version control, document review and distribution records. It was reported that policies and SOPs are reviewed on an annual basis. However, policies and SOPs do not clearly record the next review date.

Priority Recommendation: Low.
Ensure all policies consistently incorporate the annual cycle of and responsibility for review, the next scheduled date for review.

Management response: Accepted

Owner: HOIM
Date for implementation: January 2018

a23. IT topic-specific related policies and SOPs are created by PSoS. The PSoS policies and SOPs are jointly owned and apply to both PSoS and SPA. The IMT has no input on the content of jointly owned policies and SOPs.

Priority Recommendation: High.

Policies and SOPs that apply to both SPA and PSoS should be reviewed by the IMT to ensure the content is fit, for purpose, consistent and align with SPA's policies and SOPs.

Management response: Accepted.
This is part of ongoing dialogue between PSoS and SPA HR, i.e. that policy and procedure has been dual branded, but there has been no consultation with SPA in terms of content.

Owner: PSoS
Date for implementation: April 2018.

a24. The Forensic Services team has developed a number of departmental specific policies and SOPs which make reference to information management. SOPs developed include Operational Procedures for systems, Laptop Care and Deployment at Scenes, Recording Information during Scene Examinations and Management of Portable Media Devices within Forensic Services. Specific departmental policies and SOPs have not been reviewed by IMT.

Priority Recommendation: Medium.
Please see recommendation at **a23**. To ensure departmental policies and SOPs are consistent with corporate SPA policies, ensure IM is actively involved in the creation and review of SOPs relating to information security and management.

Management response: Accepted
FS will provide relevant SOPS to IM without delay, however, IM only has limited resources to review the policies.

Owner: Director of Forensic Services
Date for implementation: January 2018

a25. Corporate information security related policies and procedures are made available to staff via the IMT webpage on the staff intranet. It was reported that staff also have access to the PSoS intranet to access jointly owned IT related policies and SOPs.

Priority Recommendation: Medium.
To ensure all SPA staff are aware of their information security responsibilities, relevant dual branded PSoS policies and SOPs should be identified and made available on the SPAs intranet webpage**.**

Management response: Rejected.

a26. Forensic Services departmental policies and SOPs are made available via Q pulse. It was reported that corporate information security related policies and SOPs are also included on Q pulse for staff within Forensic Services to access. IMT do not notify Forensic Services of any updates to corporate information security related policies. There is a risk that staff within the department are referring to corporate policies which are out of date.

Priority Recommendation: Low.
To prevent the risk of staff within Forensic Services referring to outdated information security and data protection related policies and SOPs, ensure a direct link to the to corporate policies and SOPs is provided.

Management response: Rejected

a27. There is no requirement for employees to sign a declaration to confirm that they have read and understood the information security and data protection policies.

Priority Recommendation: High.
Ensure induction checklists include the key information security policies and SOPs that new starters are expected to read, in order to facilitate compliance. To ensure staff are aware of, and agree to, their information security obligations and responsibilities mandate that all permanent, temporary and contract staff, sign an agreement to confirm that they have read and understood all information security related policies and SOPs.

Management response: Accepted.
FS will work with the HOIM to explore the use of the process highlighted in the previous recommendation and whether this could be extended across the organisation

Owner: HoIM
Date for implementation: November 2018

a28. There is no formal policy or SOP approval process in place. It was reported by the HoIM, that policies or SOPs may be reviewed by the Director of Assurance and Governance and the Senior Management Group.

Priority Recommendation: High.
Ensure policies and SOPs created are reviewed and formally approved by senior management. Once a process has been agreed for policy approval, create a procedure which outlines the agreed process to staff. Timeframes in which policies

or SOPs should be signed off should be defined to ensure policies are promptly approved, implemented and disseminated to staff.

Management response: Accepted

Owner: CEO
Date for implementation: Senior Management Group will now approve Dec 18.

Mobile and Remote Working

a29. The Remote Working policy acknowledges the additional risks and vulnerabilities associated with home or remote working and sets out guidance for staff regarding the use of laptop/personal computers, mobile phones, blackberries, storage and use of equipment, transporting documents, disposal and action to take in the event of loss theft of mobile devices.

a30. In addition to the Remote Working Policy, Forensic Services has also created additional policies and SOPs for Scene Examiners. The guidance relates to Laptop Care and Deployment at Scenes, Recording Information during Scene Examinations, Management of Portable Media Devices within Forensic Services and the use of the Image Management System.

a31. It was reported user requests for the issue of mobile and remote devices are submitted to ICT on a service request form through IT Connect. Mobile devices include Laptops, USBs, mobile telephones and Blackberry devices. Requests for the issuing of mobile devices must be endorsed by the user's line manager and requestors must be able to demonstrate a business need for the device or to work remotely. It was reported that IMT is responsible for authorising the issuing of mobile devices and remote working.

a32. Laptop devices issued to users are encrypted. When the device is switched on, users are presented with a Bit Locker notification in which they are required to enter a password for the encryption. Once the RAS token is inserted users are prompted for a username and password to access the desktop. It was reported that passwords on remote devices are not changed unless a member of staff has left the organisation or there has been a theft or loss of device.

Priority Recommendation: High.
Enforce regular password changes as needed for remote devices.

Management response: Rejected.

a33. It was reported that all laptop devices are installed with Symantec anti-virus and malware detection software. In the event of an incident detected, it was

reported that a notification alert is sent to the IT service desk and Technical and Audit Assurance Manager.

a34. Blackberry devices issued are restricted to making calls and accessing work emails. Devices are password protected and expire every 30 days. Devices are configured to remind users that the password to the device is about to expire if not changed.

a35. SPA does not have a mobile device asset register which records all mobile devices provided to SPA that could be used to process personal data e.g. laptops, USB sticks and mobile phones and allocated owner of device.

Priority Recommendation: High.
Create a mobile device asset register which records all mobile devices in use by SPA.

Management response: Accepted

PSoS have failed to respond to our requests for their position on the recommendations. As such, SPA have decided that we will try and muster all our mobile assets and create our own register.

Owner: PSoS
Date for implementation: March 2018

a36. Users are not provided with specific training regarding the use of mobile devices and their responsibilities. Users are not required to sign a user agreement when issued with remote devices.

Priority Recommendation: High.
Training should be implemented for personnel using mobile devices to ensure they are aware of their responsibilities when using devices, and to raise awareness of the additional security risks resulting from remote working and the security controls that should be implemented. Once trained and prior to issuing mobile devices to personnel, ensure users have signed a user agreement acknowledging their duties and responsibilities when using mobile devices.

Management response: Accepted
SPA IM do not always know who has been allocated such devices. However, once **a35** has been completed the users will be provided with training. PSoS ICT will need to agree that all requests for mobile assets, including phones, comes through SPA IM (as it should) and refrain from the current process where they take verbal requests for jobs from senior staff.

Owner: HOIM
Date for implementation: January 2018

a37. SPA does not conduct spot checks of the security of mobile devices issued.

Priority Recommendation: High.
Undertake regular security spot checks to ensure the security of mobile devices and compliance with the Remote Working Policy.

Management response: Accepted
As per **a35**, spot checks will commence after we create register. SPA has been unable to do this due to the lack of asset register held by ICT. Each business area will assign an auditor to conduct spot checks and send reports back to HOIM.

Owner: HOIM
Date for implementation: March 2018

a38. Line Managers are responsible for the collection of mobile devices from a staff member leaving the SPA. Auditors were not provided with evidence to demonstrate that this practice was carried out by Line Managers and that the devices were returned back to IMT or ICT.

Asset Management – Responsibility of Assets

a39. Auditors were provided with annual data handling reviews conducted by SPA PQ and Forensic Services. The review records the name of protectively marked data, physical location, methods of storage, storage security, system accreditation, recipients, method of transfer, third party sharing, retention period, disposal and assessment of arrangements. Reviews date back to 2012/13. SPA does not have an up to date information asset register (IAR) which documents all physical (paper) and electronic information assets held by both SPA PQ and Forensic services located at Scottish CrIMTe Campus and across Scotland.

Priority Recommendation: High.
Create an IAR which identifies and records all information assets (both electronic and physical) held by SPA and their importance. The IAR should include information assets held by SPA PQ and Forensic Services and include the creation, processing, storage, transmission, deletion and destruction of the asset and should be continually risk assessed to ensure information assets are kept secure. Once created, the IAR should be subject to regular review to ensure it is accurate, up to date and consistent. This can be achieved by adopting a similar method and conduct data reviews of all departments within SPA.

Management response: Accepted

Owner: HOIM
Date for implementation: Work will commence November 2017

a40. Auditors were provided with a screenshot of a log recording device types. This recorded the number of docking stations, laptops, monitors, PC, iPads and encryption devices held. It is unclear if the register applies specifically to SPA and includes an accurate of all ICT assets that have been issued to SPA.

a41. SPA has only established one Information Asset Owner (IAO) who is responsible for all information assets held by Forensic Services. IAO responsibilities have been assigned to the Director of Forensic Services however; the responsibilities of the IAO were not referenced during interviews.

Priority Recommendation: High.
Ownership for all physical and electronic information assets identified should be assigned. IAOs assigned should be recorded on the corporate IAR. Roles and responsibilities of an IAO should be formally documented in job descriptions.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

Asset Management – Managing Removable Media

a42. The Management of Portable Media Devices SOP provides guidance to Forensic Services staff regarding the use of Datashur USB devices. There is no specific guidance within the IS SOP or Remote Work Policy regarding the management and use of removable media that applies to both corporate SPA and Forensic Services.

Priority Recommendation: High.
To prevent unauthorised disclosure, modification, removal or destruction of personal information stored on media, review and update the current Remote Working Policy to include guidance on the use and management of removable media, including the restrictions on the import and export of personal data via the media. Disseminate the updated policy to all staff.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a43. It was reported that desktops and remote devices have Symantec endpoint controls in place to ensure that staff cannot use unauthorised USBs. Approved encrypted Datashur USB devices can be used by staff.

a44. Staff are not required to read and sign an acceptable user agreement for the use of removable media.

Priority Recommendation: Low.
Please refer to recommendation at **a36** regarding the requirement for staff to sign a user agreement for the use of mobile device.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a45. A log of issued Datashur USB devices is maintained by ICT to identify the site location of USB devices. The log applies to USB devices issued to both SPA and PSoS locations and records serial number, device ID, issued to and location.

a46. It was reported that it is for the specific business area to maintain a list of who the specific USB devices have been issued to. Whilst it was reported that Forensic Services within the Scottish Crime Campus maintain a log to record when a member of staff has signed out and in a USB device, Auditors were unable to gain assurance that this practice is in place across SPA in Scotland. No USB audits have been carried out by SPA.

Priority Recommendation: High.
Ensure a USB log is maintained which documents the USB devices used by SPA, the location they have delivered to, the name of the individual who has been allocated the USB and date returned where appropriate.

Management response: Accepted

Owner: HOIM
Date for implementation: November 2017

a47. The IS SOP states that all CDs/DVDs containing personal data must be encrypted. Staff have read-only access to CDs on desktops.

a48. SD cards are used by Forensic Services to take photographs as part of a scene examination. SD cards are held in a secure lockable office and a log is maintained to identify the staff member that has a particular SD card.

a49. It was reported that the content of the SD card is uploaded onto the Scene Examiner's laptop once the scene investigation has been completed. Once uploaded, the content is erased. However, it was reported that data held on older SD cards used by the department may be recoverable once erased.

Priority Recommendation: High.
To prevent unauthorised access to data held on SD cards, ensure new, up to date SD cards are used. All data on SD cards should be wiped and securely destroyed to prevent the data from being recoverable.

Management response: Accepted

Owner: Head of Scene Examination
Date for implementation: December 2017

Access Control

a50. SPA does not have an Access Control Policy in place that sets out the business requirements for access control to limit access to personal information and information processing facilities. The IS SOP includes brief information in relation to requesting access to networks and systems, authorisation and auditing access controls.

Priority Recommendation: High.
Create an Access Control Policy or SOP which provides clear guidance to Line Management and staff regarding the processes to follow when requesting ICT user access or physical access to the building for new starters. For staff that change roles or leave SPA employment, the policy or SOP should include procedures for amending or removing unnecessary access permissions to the network and individual systems/applications and physical access to buildings to help ensure that staff are only able to access information on a 'need to know' basis and access is removed in a timely fashion. Once created the Policy or SOP should be regularly reviewed.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a51. Prior to the setup of a new starter's account, it was reported that the individual is required to be vetted. SPA's Human Resources (HR) department is required to advise Line Managers when vetting has been completed before a request to access the network and systems is submitted. However,

communication between departments within SPA and HR in relation to starters, movers and leavers is poor and inconsistent.

Priority Recommendation: High.
Please refer to recommendation at **a50.** Ensure the Access Control Policy or SOP includes the requirement for HR to notify the new starter's Line Manager once their vetting has been completed to enable the Line Manager to proceed with requesting an account to be setup.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a52. Line Managers are responsible for submitting new user access requests through IT Connect. This provides new users with access to the network and basic systems. The process applies to staff across SPA corporate and Forensic Services. Once the request is submitted through IT Connect, IMT are responsible for authorising the request before it reaches the IT services delivery team.

a53. Where users require access to additional applications/systems which are not included in the basic set-up it was reported that an additional request has to be submitted through IT Connect to arrange access.

a54. There is no guidance which indicates what job roles are permitted access to specific networks and systems. It was reported that new user accounts are set up by mirroring an account of a similar job role.

Priority Recommendation: High.
To control user access and to ensure users are only provided with access to networks and systems that are relevant to their specific job role. IAOs/system owners should determine which job roles that require access to the information systems/assets they are responsible for. This should be formally documented and kept under review.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a55. Line Managers are responsible for notifying HR of any leavers within their department. However, as mentioned at **a51**, communication between HR and SPA departments is poor and inconsistent.

Priority Recommendation: High.

Ensure the leavers and movers procedure documented within the Access Control Policy or SOP sets out the requirement for Line Managers to notify HR of any leavers or movers within the department. Please refer to recommendation at **a50**.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a56. HR are responsible for notifying ICT of any leavers/movers and the leave date. Accounts are scheduled to be disabled at the end of the last working day. Data on user accounts is retained for 90 days and backed up for a further 90 days. All data is deleted after the specified timeframe if no request to retain data has been submitted by Line Management. However, as mentioned at **a51**, there are concerns regarding communication between departments.

Priority Recommendation: High.
Please refer to recommendation at **a51** and **a52** to ensure controls are in place to improve communication between departments.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a57. Where a member of staff moves department within SPA, Line Managers are required to notify ICT of any systems the user no longer requires access to. However, it was reported that ICT are not always notified of users moving departments. As such, there is a risk that users have access to systems and applications that are no longer required for the purpose of the current job role.

Priority Recommendation: High.
In addition to the policy or SOP recommended at **a50**, create a new starter/movers/leavers checklist, which provides guidance to Line Managers on the steps that should be taken in the event of a staff member joining, moving or leaving the department. This should include the requirement to notify HR and ICT.

Management response: Accepted

Owner: Records Manager
Date for implementation: December 2017

a58. Regular reviews of users' access rights are not carried out across SPA.

Priority Recommendation: Urgent
Ensure regular proactive monitoring of information systems access through random dip samples of access attempts. Access rights should be audited regularly to ensure that individuals with no right of access to specific systems or applications are removed.

Management response: Accepted

Owner: Records Manager to identify department leads. FS to identify their leads
Date for implementation: Quarter 1 2018

a59. Additional applications/systems used by Forensics Services include the Electronic Management System (EMS), Image Management System (IMS) and Q pulse. Access to applications requires the users to enter an additional username and password to access case files held on the applications.

Physical Security

a60. Physical security risk assessments of protectively marked assets are not carried out by IMT. It was reported that physical security risk assessments are only conducted when there is a significant change; however, assessments are not formally documented.

Priority Recommendation: Urgent.
To ensure the protection of protectively marked information assets, ensure regular physical security risk assessments are carried out by the IMT. Assessments should include physical access to building, passes, reception area, visitor's procedures, location of equipment that can access criminal databases, locks on offices or areas processing personal data, shared office area and vetting levels of staff. Physical security assessments should be formally documented for audit and monitoring purposes. Recommendations as a result of assessment should be followed up to ensure appropriate controls have been implemented.

Management response: Rejected

ICO comment:
SPA has challenged the accuracy of this finding and have claimed that physical security risk assessments are carried out; however, no evidence was provided to Auditors to support that assertion.

a61. No physical security risks assessments have been carried out at the Scottish Crime Campus in Glasgow or Forensic service premises across Dundee, Edinburgh

or Inverness. Access to physical records e.g. fingerprints, crime scene images and applications such as the Criminal History System (CHS) and DNA system is accessible at these sites.

Priority Recommendation: Urgent.
Please refer to recommendation at **a60**.

Management response: Rejected

a62. SPA has a Physical and Environmental Security Policy in place to ensure the protection of SPA staff and premises. The Physical and Environmental Policy includes information on response and threat levels, management of threat, security awareness and control of access to the building; this includes enforcing a pass system.

a63. Auditors were provided with the opportunity to have a brief tour of SPA PQ. They are co-located with Disclosure Scotland. CCTV is situated around the premises and inside the building which is monitored by the security team at the main building reception. Building security is provided by third party Cordant Security.

a64. To enter the building, staff at both SPA and Disclosure Scotland, are required to swipe their staff ID badge and enter a four digit pin. It was reported that pins are unique to the individual staff member and only changed in the event a staff member loses their identity badge or forgotten their allocated pin number.

a65. Disclosure Scotland are responsible for issuing SPA staff with access badges and pins to access the building. Appropriate access controls are in place to prevent unauthorised access to SPA's office area by a member of staff from Disclosure Scotland. SPA badges are configured to allow access to SPA office area and Canteen only.

a66. Visitors entering the building are required to buzz at the office entrance to notify security which organisation and member of staff they are visiting. Once entrance to the building has been permitted, visitors are required to sign in and out at reception and provided with visitor badges to be worn at all times.

a67. SPA is located on the second floor of the PQ building. To access the office area, staff are required to swipe their badges. Where the security controls are raised due to the changes to the threat level, additional security measures may be activated which requires staff to swipe their identity badge and enter their unique 4 digit pin.

a68. Regular physical access control audits to PQ are not carried out by the IMT.

Priority Recommendation: High.

Proactively conduct physical access control audits to ensure staff only have access to the permitted areas of the building. Conducting regular physical access control audits will also assist SPA with identifying staff that are still registered to have access to the building but have left the organisation.

Management response: Accepted

Owner: HOIM
Date for implementation: November 2017

a69. It was reported that SPA PQ operate a clear desk policy, this is referenced within the IS SOP. All documents are required to be locked away in draws located underneath desk areas. However, spot checks are not conducted at the end of a business day to ensure staff compliance with the clear desk policy.

Priority Recommendation: Urgent.
Ensure the clear desk and screen procedures are communicated to all staff and any relevant third party contractors and home/remote workers.
Line Managers and the IMT should carry out spot checks at the end of the business day to ensure personal data has not been left unattended and staff adherence to the clear desk policy. Printers should be checked to make sure information is not left unattended during the day or overnight. Staff should also be told to lock their workstations using "ctrl-alt-delete" when not in use and monitor compliance. Spot checks should be formally documented for audit and monitoring purposes.

Management response: Accepted

Owner: IM/Line Managers
Date for implementation: November 2017

a70. Auditors conducted a brief tour of the office premises to assess the security controls in place. All desks had been left unattended as all staff were attending a board meeting.

a71. Whilst touring the SPA office area, Auditors observed HR documents relating to meetings, staff consultations and health retirement reports left unattended on filing cabinets; reports dated back to 2014.

Priority Recommendation: Urgent.
Documents containing personal or sensitive personal data should be stored in a secure room, or a lockable filing cabinet or unit. Keys to offices or filing cabinets should be held in a secure key safe within the department. Access to information should be restricted on a need-to-know basis only.

Management response: Accepted

Owner: Records Manager
Date for implementation: Tbc

a72. Legal case files containing personal data were left unattended on top of cabinets and draws containing additional legal files were left unlocked. Storage boxes containing further legal case files were situated underneath desks.

Priority Recommendation: Urgent.
Please refer to recommendations at **a69** and **a71**.

Management response: Accepted

Owner: Head of Legal
Date for implementation: Complete in terms of securing the files

a73. Auditors were provided with access to the Chair of the Board's office to conduct interviews during the onsite visit. The unattended desk had not been cleared of personal data or mobile devices and we observed a laptop, RAS token, desk drawer keys, a restricted document with login and password information for remote/mobile working and a number of other emails and letters containing personal data. There is a clear risk of unauthorised access to the documents but also the laptop and SPA network. The incident was reported to the RM but it is not known if this or the other security incidents mentioned during the tour were logged as security breach incidents.

Priority Recommendation: Urgent.
Please refer to recommendation at **a69** regarding reinforcing clear desk policy. Review the current guidance in the Handbook regarding password complexity rules to include password rules regarding the management of passwords.

Management response: Accepted

Owner: HOIM
Date for implementation: November 2017

a74. End of life IT equipment or returned mobile devices are held in the IMT's office. It was reported that requests have been made for ICT to collect equipment for secure destruction but it remains uncollected. It was reported that the office is locked at the end of the business day.

Priority Recommendation: High.

Ensure all end of life IT equipment is collected and securely destroyed. The Asset register should be updated accordingly to record the destruction of old equipment.

Management response: Partially Accepted
IM staff will now put on ICT requests to have kit collected, however, the update of the central asset register after destruction is a matter for PSoS, not SPA. SPA can update its local register for mobile devices only.

Owner: HOIM/ICT
Date for implementation: Implemented

a75. There are confidential waste consoles located around the office. Shred It are the third party contractor responsible for disposing of the confidential waste by shredding onsite every two weeks. The security team is responsible for collecting confidential waste sacks from the consoles. Sacks are stored within a locked storage room situated on the ground floor. Auditors were unable to confirm if destruction certificates are obtained that correspond with the amount of waste collected for destruction.

Priority Recommendation: High.
Where a third party is used to dispose of confidential waste, ensure certificates of destruction are obtained to gain assurance that confidential waste has been securely destroyed.

Management response: Accepted.

Owner: HoIM
Date for implementation: December 2017

a76. SPA PQ has secure print facilities; each person has their own unique username and pin to allow them to access and collect their prints.

a77. Auditors also conducted a brief tour of the Scottish Crime Campus. Similar to PQ, staff are required to swipe badges to enter the premises. Access to areas within the building is role based and staff are required to swipe ID cards to access areas. A spreadsheet of physical access to building required by each role is maintained to identify the access a new starter will require.

a78. It was reported that leavers are required to return staff passes to be destroyed. In the event a pass is not returned, the pass can be deactivated to prevent access to the building. However, this process requires Line Managers to notify security to deactivate the pass. Regular physical user access audits are not conducted at the Scottish Crime Campus.

a79. For visitors, staff are required to inform security of any visitors scheduled to visit the premises. Security maintains a list of expected visitors and access to building is permitted once the visitors name is confirmed. Visitors are required to sign in at reception where they are provided with a photo ID badge.

a80. It was reported that the Scottish Crime Campus operate a clear desk policy; however, this was not carried out in practice and no spot checks were conducted.

Priority Recommendation: Urgent.
Please refer to recommendation at **a69**.

Management response: Partially Accepted
Spot checks are conducted, however, it is accepted that from time to time there are some documents appearing. This has been taken on board and checks will be conducted more frequently and reminders issued regularly

Owner: Director of Forensic Services
Date for implementation: Complete

a81. It was reported that all files are stored away at the end of a business day and all departmental filing cabinets are locked. This is the responsibility of the last member of the team in the office. However, whilst conducting the tour, Auditors observed storage boxes recalled from archive stored beside the office desks. The storage boxes contained information relating to a murder case file. The team within the area were no longer in the office and boxes had been left unattended.

Priority Recommendation: Urgent.
Please refer to recommendation at **a71**.

Management response: Accepted
A review of storage is already underway as it is accepted that more storage is needed for when files are recalled from storage. Key boxes in situ and temporary storage freed up in the interim.

Owner: Director of Forensic Services
Date for implementation: Complete

Supplier Relationships

a82. As previously mentioned, ICT services is outsourced to PSoS. SPA does not have a formal written agreement in place with PSoS which clearly sets out the relationship between SPA and PSoS, services that are provided and clear instructions to be followed by PSoS.

Priority Recommendation: Urgent.
Please refer to recommendation at **a8**, within 'Information Security – Organisation' regarding the creation of a written contract. Information security requirements should be established and agreed with PSoS within the written agreement. The following terms should be included for inclusion within the contract to address information security requirements; description of data accessible, legal and regulatory requirements (DPA), obligation by PSoS to implement an agreed set of access, monitoring and reporting controls, rules of acceptable use of information, explicit list of supplier personnel authorised to access SPA information, incident management, training and awareness and right to audit.

Management response: Accepted.
Agreed as part of the whole agreement that needs to be documented with PSoS with the temporary legal resource that we are hiring

Owner: Director of Governance & Assurance
Date for implementation: April 2018

a83. A Section 83 (Police and Fire Reform (Scotland) Act 2012) agreement was created by the SPA's HoLC, alongside their counterpart at PSoS. This agreement attempted to detail all the services provided to SPA by PSoS but has yet to be finalised and signed off.

a84. SPA's procurement process is managed by the PSoS Procurement Department. All written agreements with third parties are drafted in the name of SPA. This applies to formal agreements for both SPA and PSoS.

a85. SPA does not have a third party supplier relationship information security management policy or SOP which documents the processes to follow to ensure appropriate security controls have been identified and implemented when dealing with suppliers handling personal data processed by SPA.

Priority Recommendation: Urgent.
An Information Security Management Policy or SOP for supplier relationships should be created. This should identify information security controls to address supplier access to information (Please refer to recommendation at **a82** regarding controls that should be included). The processes and procedures to be taken when entering into an agreement should be set out. Creation of a policy or SOP would ensure a consistent approach is adopted throughout SPA when entering into a supplier agreement.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
SPA were unable to provide the ICO with an indication of the date by which this recommendation is to be implemented and what steps will be taken to ensure compliance due to a lack of response from the PSoS.

a86. When a supplier is required to provide services for SPA, an Invitation to Tender (ITT) is sent out. The ITT includes a security aspects letter which outlines the security measures that should be in place. The security aspects letter includes checks on the encryption they have and whether they vet any employees. Auditors were provided with an ITT for Interim Payroll Solution, it was unclear whether this related to SPA or PSoS.

a87. Auditors were informed that the relevant Information Security Officer for either SPA which is the HoIM or PSoS would be involved in drafting the security aspect letter, reviewing and scoring the information security requirements provided by third party suppliers, carrying out PIAs and reviewing the drafted contract. Details of the evaluators for the Interim Payroll Solution for PSoS were provided. No evidence was provided to show that the HoIM was involved in the ITT and it was reported that SPA HoIM has only reviewed two contracts this year and has not been involved in any ITT.

Priority Recommendation: Urgent.
To ensure SPA has oversight of all ITT, ensure the HoIM at SPA is involved in the ITT process and drafting of supplier contracts to review to ensure all information security requirements have been addressed and included in the contract.

Management response: Accepted.

Owner: PSoS/Director of Governance
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a88. Whilst the supplier staff who will be involved in providing the services are required to be vetted, neither the ITT nor the security aspects letter requires contractors to provide staff with appropriate information security training.

Priority Recommendation: High.
To ensure suppliers' staff are aware of their responsibilities when handling protectively marked information, require suppliers to deliver information security

training to staff. Evidence of the delivery of training should be requested from suppliers to gain assurance.

Management response: Accepted.

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a89. The security aspects letter includes the requirement for suppliers to notify PSoS Information Security Officer (ISO).There is no reference regarding the requirement to notify the HoIM at SPA. There is a risk that HoIM will not be made aware of security incidents reported by third party suppliers.

Priority Recommendation: High.
Where the third party supplier contract relates to the processing of SPA's personal data, ensure the written contract includes the requirement for the third party to report all information security incidents to the HoIM at SPA. The contract should include clear instructions for the third party supplier to follow when reporting a breach. Contact details of SPA's HoIM should be included within the contract.

Management response: Accepted.

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a90. Auditors were only provided with one example of an ITT and security aspects which made specific reference to PSoS rather than SPA. Auditors were not provided with a finalised supplier contract and were unable to gain assurance that the current process reported is consistent throughout SPA.
Priority Recommendation: Urgent.
Please refer to recommendation at **a85** regarding the creation of an Information Security Management Policy or SOP for Supplier relationships and **a87** regarding SPA oversight of all supplier relationship agreements.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a91. The security aspects letter states that throughout the life of the contract, compliance with all of the security provisions shall be monitored by PSoS. There was no reference made to SPA and the right to conduct audits of third party supplier to ensure compliance with the requirements specified within the formal agreement.

Priority Recommendation: High
Ensure that the contracts include the right for SPA to conduct regular audits. Conduct regular supplier audits to ensure compliance with the security requirements set out within the contract. Audits should be formally documented for monitoring purposes.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a92. Auditors briefly viewed the contract log on site. It captured information relating to the contract type, contract length and department responsible for the contract.

Incident Management

a93. SPA does not have an overarching Incident Management Policy. There is information on reporting information security incidents in the IS SOP. However, the guidance makes specific reference to network and system security incidents, there is no reference to the reporting of physical information security incidents.

Priority Recommendation: High
Develop an Information Security Incident Management Policy, setting out roles and responsibilities for managing information security incidents, detailing how to identify and report an incident, and signposting where to seek further guidance. Publicise the policy to ensure staff awareness of their information security incident management responsibilities. Consider creating an incident reporting form on SPA's intranet that staff can use to report information security incidents.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a94. The IS SOP requires staff to complete the incident reporting form included within the appendix and to their Line Manager or IMT within 24 hours of the incident occurring or being discovered. There was a lack of staff awareness of the IS SOP or the incident reporting form contained within the appendix and staff interviewed reported that they would report information security incidents verbally to both Line Management and IMT.

Priority Recommendation: High
Please refer to recommendation at **a97**.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a95. Identified information security incidents within Forensic Services are recorded as non-conformities on the Q Pulse system. Auditors were provided with a non-conformity record which includes details of the non-conformity and escalation. All information security incidents are classified as critical escalated to the Head of Function. Action taken is dependent upon the severity of the incident. In the event of a severe breach, it was reported that a Gold Group meeting would be arranged to discuss and resolve the incident. Whilst it was reported that in the event of a Gold Group meeting that IMT will be contacted to attend, it was unclear how all information security incidents reported within Forensic Services and reported to IMT.

Priority Recommendation: High
Create a procedure for all business areas within SPA to formally record and report information security incidents identified centrally to IMT. Centralising the reporting mechanism would ensure all information security incident are effectively reported, logged and management by IMT to prevent further incidents. The procedure should be included in the Information Security Incident Policy recommended at **a93**.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a96. Cyber related security incidents must be reported to the IT helpdesk team who operate on a 24/7 basis. The Technical Assurance team are responsible for investigating all cyber related incidents. For any security incidents that are detected by the system, the Technical Assurance Manager receives an incident alert via email or SMS, this includes outside office hours.

a97. IMT is responsible for investigating information security incidents within SPA. There is no guidance on how to manage an information security incident or when it is appropriate to report to the ICO.

Priority Recommendation: High.
A procedure which provides guidelines to staff responsible for investigating security incidents should be created. The document should include the process to follow once a security incident report has been received, risk assessing the potential harm and distress, logging and circumstances in which security incidents may need escalating or reporting to external bodies e.g. ICO.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a98. IMT are not notified of any information security incidents that have been brought to PSoS' ISO. For example, Titus, the system that prevents staff from sending restricted documents to private email addresses incurred an error which caused the control to shut down. IMT was not immediately notified of the incident and it became evident that during this period staff had sent restricted documents to private emails addresses.

Priority Recommendation: High.
Please see recommendation at **a93** and **a95** regarding the creation of a formal procedure which is included in the recommended Information Security Incident Management Policy to centralise reporting from all business areas including PSoS to IMT.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

a99. A security incident log is maintained by SPA. This includes date of incident, incident type, details, risk category and lessons learned.

a100. Lessons learned from security incidents are not communicated to staff across SPA.

Priority Recommendation: High
Lessons learned from analysing and resolving a security incident should be communicated to staff to reduce the likelihood or impact of future security incidents.

Management response: Partially Accepted
The lessons learned are not always relevant for dissemination to staff.

Owner: HOIM
Date for implementation: As required

a101. It was reported that the Director of Finance is responsible for providing security incident breach reports to the Committee on a quarterly basis. The security incident report is compiled by IMT. Auditors were provided with a Recent Incidents – ICT report which was delivered to the Committee by the PSoS Director of ICT. The purpose of the report was to inform the Committee of the high impacting IT incidents. Auditors were not provided with evidence to support that all physical (paper) and IT related information security breaches are reported to the Committee.

Priority Recommendation: High
To ensure senior management within SPA have appropriate oversight, ensure both cyber and physical related information security incidents are reported to the Committee. Reports should explain the security incidents occurred within the quarter, the severity of the incidents, action taken to resolve/mitigate the incident and escalation.

Management response: Accepted.

Owner: CEO/Audit Committee
Date for implementation: January 2018

Compliance – Information Security Reviews

a102. SPA's Data Protection Policy states that an audit plan based on a risk assessment should be created by SPA. It was reported that an audit plan is agreed with external auditors and is approved by the board.

a103. Scott Moncrieff are responsible for providing an audit function for SPA. It was reported that an audit for 2016/17 was completed and a draft report was

provided to the Committee in July 2017. Specific information security compliance was not addressed.

Priority Recommendation: High.
SPA should conduct regular information security audits to assess compliance with relevant policies and procedures. Audit reviews should ensure the continuing suitability, adequacy and effectiveness of SPA's current approach to information security.

Management response: Accepted.
We were just getting agreement on resources for this. We are going to use our external auditors.

Owner: CEO/Audit Committee
Date for implementation: April 2018

a104. PSoS is responsible for arranging and conducting technical compliance audits of the ICT system. NTA Monitor Ltd were contracted to carry out an IT Health check on SPA systems. The report stated that there were 20 high, 30 medium and five low risk issues identified. Whilst the report was provided to Auditors by PSoS as a result of the Audit, IMT have not been provided with the report. No management response or action plan resulting from this health check was provided.

Priority Recommendation: High.
Create an action plan and ensure that the recommendations from the IT Health Check are implemented. Please also refer to recommendation at **a8**.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

a105. It was reported that HoIM and PSoS ISO are jointly responsible for ensuring the accreditation of the SPA network and information systems. No evidence of any assessments of SPA systems was provided.

a106. It was reported that some management compliance reviews are undertaken by IMT, for example, by using MailMarshal to check the use of insecure email addresses.

a107. Management compliance reviews of systems and processes within their areas, spot checks to ensure compliance with relevant IS policies and SOPs are not formally carried out and documented. Staff surveys are not conducted across SPA to assess staff awareness regarding information security when handling personal data.

Priority Recommendation: High.
Create a programme of spot checks and/or staff surveys to assess and promote compliance with SPA's information security policies and procedures.

Management response: Accepted

Owner: HOIM/Records Manager
Date for implementation: 1st Quarter 2018

a108. HoIM is responsible for liaising with the PSoS's ISO to arrange vulnerability assessments and penetration testing for SPA. Recommendations are provided by the HoIM with regards to the systems that should undergo a vulnerability assessment or penetration test. However, there is a lack of communication between HoIM and PSoS ISO regarding the technical compliance reviews that have been finalised and when they will be conducted. Results of reviews carried out or changes to scheduled reviews are not communicated to the HoIM.

Priority Recommendation: High.
Please refer to recommendation at **a8** and **a82** regarding the requirement to formalise the services provided to SPA to ensure oversight.

Management response: Accepted

Owner: PSoS
Date for implementation:

ICO Comment
Please refer to ICO comment at **a85**.

a109. It was reported that a full list of vulnerability and penetration tests carried out is maintained. Auditors were not provided with evidence of the record maintained.

8.2 Scope B: Training and Awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

Risk: If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the Data Protection Act 1998 resulting in regulatory action and/or reputational damage to the organisation

Recommendations	
Urgent:	5
High Priority:	18
Medium Priority:	6
Low Priority:	3

Management Structures

b1. There is no management framework in place with effective oversight of data protection and information security training.

Priority Recommendation: High.
A management framework should be put in place with a delegated process of accountability and responsibility from the board down, to ensure the effective oversight of data protection and information security training.

Management response: Accepted.

Owner: Chair of Board/CEO
Date for implementation: 1st Quarter 2018

b2. Board meetings do take place but the SIRO, HoIM or Records Manager are not invited to attend. Data protection and Information security training is not monitored or discussed at this or any other steering group or forum.

Priority Recommendation: Urgent.
Create an Information Management steering group to monitor and mandate data protection and information security training and improvements. This group should be chaired by the SIRO and include the Head of Information Management. The Steering Group should report to the Board.

Management response: Accepted.
The SIRO and HOIM support this recommendation and have discussed group membership with agreement from general business areas, however, the Board need to agree re the reporting mechanism. It is felt that, given the size of SPA

that **b2** and **a17** could be one Group that will then report to the CEO who will report to the Board.

Owner: Director of Governance & Assurance/Chair of Board
Date for implementation: February 2018

b3. SPA previously employed a Training Manager in Forensic Services who was responsible for ensuring the appropriate training needs were addressed and completion monitored. When the Training manager retired the post was disestablished.

Priority Recommendation: High.
Responsibility for DP and IS training should be allocated to an appropriate individual who will be responsible for training across the entire organisation. That person should be key in the development and implementation of the TNA and training plan.

Management response: Partially Accepted
FS will allocate resources to perform a TNA and will assist the IMT to ensure that where they deliver training to FS staff, records are updated accordingly.

Owner: HOIM/Director of Forensic Services
Date for implementation: 1st Quarter 2018

b4. The job description for the IMT specialist states that one of their responsibilities is to provide specialist Information Assurance (IA) advice and training across SPA and the wider Criminal Justice community, where appropriate; however this is not reflected in the data protection or Information Security policy.

Priority Recommendation: Medium.
Ensure the Overall responsibility for data protection and information security training is recorded in the relevant policies and corporate training plans.

Management response: Accepted.
The job descriptions are all being changed in February 2018 as a result of job evaluation.

Owner: HOIM
Date for implementation: February 2018

b5. The job description of the RM includes the responsibility to provide specialist expertise including training on records managements to SPA Officers and where appropriate PSoS. The current RM was appointed at the end of 2015.

b6. The Information Assurance Handbook is provided to staff as part of their induction, the handbook details what the IMT are responsible for and how to contact them.

b7. Forensic Services has a Training and Competency SOP which allocates responsibilities to key individuals within Forensic Services. The Heads of Function has overall responsibility for the Training and Competence System of Forensic Services. Day to day training responsibilities lie with the Operations Managers, Team Managers and Head of Administration.

b8. The HoIM takes responsibility for data protection and information security training for teams. However, this does not include Forensic Services.

Priority Recommendation: High.
Ensure all departmental data protection training is provided by the IMT to ensure consistency across departments.

Management response: Rejected

Training Programme

b9. All SPA employees including temporary and contract staff are mandated to complete the induction training on appointment. However, there is no formal data protection or information security training programme in place.

Priority Recommendation: High.
A data protection and information security training programme should be developed across the whole of SPA and should include Forensic Services. This should be approved by senior management and mandated for all staff.

Management response: Accepted

Owner: HOIM/CEO
Date for implementation: April 2018

SPA comment
CEO has now approved scoping an e-product. We would like to develop and implement a full suite of e-training. However, we will increase face-to-face and intranet bulletins in the interim.

b10. A training needs analysis has not been conducted for staff groups, including temporary or contract staff, who handle personal data. There is a risk that staff groups have not received an appropriate level of data protection and information security training.

Priority Recommendation: Urgent.
SPA needs to ensure that a Training needs analysis is completed for all staff including temporary and contract staff. This should be based on the staff member's job role and how much access to personal data they have. This will help the understanding of what training needs to be provided to staff in each department of SPA.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

b11. SPA has not developed a training plan or strategy.

Priority Recommendation: High.
SPA needs to develop a training plan or strategy to meet training needs within agreed timescales.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

Induction Training

b12. SPA provides induction training in multiple formats; Auditors were informed that the two hour induction is provided to all staff on their first day. However we were not able to gain assurance that this happened in practice. Further to this the requirement to complete induction training on the first day of employment is not documented in policy.

Priority Recommendation: High.
Document within the organisations Data Protection policy when staff members are required to complete mandatory data protection and information security training and monitor compliance.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

b13. The presentation includes guidance on data protection, information security and how to handle a subject access request, user responsibility and IMT contact details. Auditors were also informed that staff are made aware of current issues and lessons learnt from relevant security incidents.

b14. Forensics Services has their own induction training that IMT has no involvement in. Forensic Service induction includes a checklist which the Line Manager is responsible for ensuring is completed. Only a blank template checklist was provided so we were unable to establish whether it was effective. There is a section on data protection and information security including employee's responsibilities. The induction checklist is a Forensic Services owned document and forms part of the training record.

Priority Recommendation: High.
Induction checklists should be submitted centrally so Information Management have oversight of its effectiveness.

Management response: Rejected

b15. The Information Assurance Handbook is provided to staff at induction and includes a general overview of IMT and Assurance. It details staff's obligations and responsibilities. It informs staff that as well as reading the contents of this handbook, they should also ensure that they read and understand a list of policies which includes the Information security and data protection policy. However, not all staff interviewed had received a copy of this handbook.

Priority Recommendation: High.
Ensure that all staff receives a copy of the Information Assurance Handbook at induction. Staff should sign acknowledgement of this and this should be recorded on their scope record.

Management response: Partially Accepted
The Handbook was intended as an aide memoir, not an official document. However, a checklist will be drawn up for staff to sign at induction to record their agreement that they have been informed of the key relevant policy/procedure and understand that it is their responsibility to read the policy. This checklist could include 'provided with Handbook'. Need to establish how this can be recorded on Scope.

Owner: HOIM
Date for implementation: January 2018

b16. Auditors were informed that attendees were required to sign a training attendance record which should be added to the employees Scope record by their Line manager. However no evidence of this happening in practice was provided.

Priority Recommendation: Medium.
SPA should ensure that all attendees sign to confirm that they have completed induction training. The attendance record should be retained and logged on a staff member's Scope record to ensure that training is delivered to all staff including temporary contract and senior staff.

Management response: Accepted
Need to engage with HR in terms of updating scope records. FS will manage theirs locally if IM provide data.

Owner: HOIM
Date for implementation: 1st quarter 2018

b17. Auditors were informed that all staff including temporary and contract staff were required to complete induction training and this also included all grades such as senior managers. However, SPA do not produce training statistics or have KPIs and as such could not provide any evidence to support this.

b18. It was reported that historically there has been some resistance from legacy Board Members to complete induction training even though it is mandatory.

Priority Recommendation: High.
Employees at all levels including senior managers need to be aware of what their roles and responsibilities are, specifically in relation to data protection, information security and their employment at SPA. Ensure this training is mandated for all staff and senior managers should lead by example.

Management response: Rejected

b19. The induction training slides which formed part of the face to face training was written by the HoIM**.** The content of the slides are at least two years old and it was acknowledged they required reviewing and updating.

Priority Recommendation: Medium.
SPA should review and update the content of induction training on an annual basis to ensure that it remains relevant and up to date. This is especially important in light of the new GDPR legislation.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

b20. SPA does not include a test or assessment that the individual understands the training content or the effectiveness of the induction training provided for staff.

Priority Recommendation: High.
Develop a test for the end of the data protection induction training. It should have a minimum pass mark of at least 70% to provide SPA with assurances that staff have understood the content of the presentation.

Management response: Accepted

Owner: HOIM
Date for implementation: April 2018

Refresher Training

b21. SPA does not mandate any data protection or information security refresher training; interviewees confirmed that they would welcome regular refresher training and felt it would be beneficial. Concern was expressed that it is possible for a member of staff to be employed for over 10 years and not receive any additional training following the induction course.

Priority Recommendation: Urgent.
To ensure staff are up-to-date with current legislation and also with organisational developments regarding data protection and information security it is recommended that SPA introduce regular mandatory refresher training for all staff, including temporary and contract staff, at all grades. This is particularly relevant for staff who have regular access to personal data.
This will help to ensure staff remain aware of their data protection obligations and responsibilities.

Management response: Accepted

Owner: HOIM
Date for implementation: April 2018

b22. Although SPA does not provide regular mandated refresher training, SPA provided one off additional training as a result of a data breach incident in 2015.

Approximately two years ago IMT ran update sessions to all staff including Forensic Services. These sessions were to raise the profile of the IMT, information security and data protection. IMT went to all sites and 100% of Forensic Services staff attended. No figures were available to confirm what percentage of SPA staff attended, nor have these sessions been repeated.

Priority Recommendation: High.
Refresher training sessions should be delivered to all staff on a regular basis. The contents of any refresher training should be approved at an appropriate level and delivered to all relevant staff including temporary and contract staff. Refresher training can be bespoke and relevant to individual teams.

Management response: Accepted

Owner: HOIM
Date for implementation: April 2018

b23. At the same time, to ensure all staff were captured in the training, the HoIM asked HR for a list of people on long term sick or maternity leave and sent them a copy of the training presentation and IMT handbook. Some staff wrote back saying that they no longer worked for SPA.

Priority Recommendation: High
SPA should develop a starter, movers and leavers process to ensure that their records are accurate and up to date and that only relevant staff are provided access to SPA information and systems.

Management response: Accepted.

Owner: PSoS
Date for implementation: Tbc

ICO comment
Please refer to ICO comment at **a85**.

b24. As a result of the same incident, Forensics Services created a bespoke training package via PSoS Moodle eLearning training network, for which they have access. This training included elements of data protection and information security. This training is monitored with a test pass rate set. All staff were required to complete this training approximately two years ago. It has not been refreshed. Auditors were unable to view Moodle on site as no one interviewed had the access rights and the screenshots provided could not be opened and viewed. Auditors were therefore unable to make an assessment on how adequate and effective this training was.

Priority Recommendation: Medium.

SPA should grant access to Moodle across the entire organisation to ensure the same level of training is accessible for all staff.

Management response: Accepted

Owner: HOIM
Date for implementation: January 2018 (to include new DP legislation training)

Specialised Training

b25. SPA has not identified which members of staff require specialist data protection training to carry out their role effectively.

b26. The current interim SIRO and IAO have not received any specialist training in order to carry out their roles effectively. However, the SIRO has had data protection training in previous roles.

Priority Recommendation: High.
SPA should ensure that all staff that require specialised training are appropriately identified through a TNA and trained as necessary. SPA should also use or make reference to, relevant ICO statutory guidance/codes of practice, where appropriate.

Management response: Accepted

Owner: b25-HOIM, **b26**-CEO
Date for implementation: Tbc

b27. IMT receive approximately eight subject access requests (SAR) each year, no specialist SAR training is provided. However, it was confirmed that there is no checklist within IMT to ensure a consistent approach when responding to SARS. The majority of staff interviewed confirmed that they knew to refer requests to their Line Managers or IMT.

Priority Recommendation: Low.
Develop a checklist to ensure a consistent approach when responding to requests.

Management response: Rejected

b28. IMT confirmed that more training is necessary as some staff do not know the difference between a SAR and Freedom of Information (FOI) request.

Priority Recommendation: High.
Ensure staff are fully trained in recognising a request for information so that those requests are referred to the correct department and responded to within the statutory timeframe.

Management response: Accepted

Owner: HOIM
Date for implementation: January 2018

b29. The HoIM has the ISEB qualification in both Data Protection and Information Security, has worked in data protection since 1996 and is a BS7799 Lead Auditor.

b30. The HoIM and the RM proactively enrol on free external training, including courses on the GDPR.

Staff Awareness

b31. The training department has been disestablished; previously they would coordinate feedback from delegates. No evidence could be provided that feedback is requested from staff after completing any data protection or information security training.

Priority Recommendation: Medium.
Allow staff the opportunity to provide feedback on the induction training and refresher training to identify any key themes that can be incorporated into the training.

Management response: Accepted

Owner: HOIM
Date for implementation: January 2018

b32. SPA's intranet includes an IMT webpage which can be accessed via the home page through 'departments'. This page includes all the relevant policies and procedures, services and contact details. The majority of staff interviewed were aware of where they could go for guidance but IMT acknowledged that these pages need to be improved.

Priority Recommendation: Low.
Improve the Information Management intranet page for staff to visit for advice. If not already available, staff should be able to find advice for a range of data

protection issues, such as security, data incident management, SARs, information sharing, fair processing and exemptions.

Management response: Accepted

Owner: HOIM
Date for implementation: 1st quarter 2018

b33. The email system is used to communicate to staff updates in policies and procedures and to raise awareness of personal and information security. Forensic Services use a document management system called QPulse. QPulse requires Forensic Services staff to acknowledge any outstanding, new or amended documents. This would include data protection and information security policies.

Priority Recommendation: Low.
SPA should consider implementing the Q Pulse system or similar throughout its other departments to ensure staff have read new or amended policies and procedures.

Management response: Partially Accepted.
The FS quality manager will look at the possibility of using Q Pulse across the estate.

Owner: Director of Forensic Services/HOIM
Date for implementation: 1st quarter 2018

b34. IMT run a programme of 'Hot Topics' on an adhoc basis explaining who they are and what they deliver to the organisation. These 15-20 minute sessions have included data protection and information security incidents.

Suggestion:
Consider running the 'Hot Topics' sessions across SPA for all staff to attend, it would be good practice to include their attendance on the scope record.

b35. Auditors observed posters displayed above printers and posters at the entrances reminding staff to wear identity badges as well as Home Office and CPM posters.

b36. SPA produces and circulates a newsletter called 'The Visitor'. The HoIM has contributed to articles about data protection and information security and has provided copies as evidence. We were unable to confirm how often the newsletter is published and circulated.

Monitoring or Reporting

b37. There is no requirement to monitor and report on the uptake of data protection and information security training.

Priority Recommendation: Urgent.
SPA should implement a mechanism to monitor staff completion of mandatory training. This will allow SPA to identify staff that need to complete induction or refresher training.

Management response: Rejected

b38. The completion of induction training for SPA staff should be recorded on their scope record which is an electronic record of training held by HR. Line Managers are responsible for updating individual scope records but they are not centrally monitored. Auditors were informed that in practice the scope training records may not consistently be kept up to date.

Priority Recommendation: High.
SPA should ensure that training completion is accurately recorded on staff scope records and kept up to date.

Management response: Accepted

Owner: Line Managers
Date for implementation: December 2017

b39. In Forensic Services, personal training records are monitored by Line Managers every six months, and annually by their accreditation body, United Kingdom Accreditation Services (UKAS). However, there is no requirement to report this to the IMT, or to any other steering group or forum.

Priority Recommendation: High.
Forensic Services training statistics should be regularly provided to Information Management to ensure that there is central oversight of data protection and information security training.

Management response: Rejected

b40. SPA does not currently have a performance framework or KPIs in place for data protection and information security training completion and do not currently report on any data protection or information security training.

Priority Recommendation: High.
KPIs should be agreed and statistics should be produced on a monthly basis in order to actively monitor SPA performance to training completion.

Management response: Rejected
SPA has a huge burden in terms of training, particularly in forensics. It would be completely unrealistic to have KPI's for all training

b41. Data protection and information security training objectives do not form part of the annual appraisal process as there is no formal training programme in place.

Priority Recommendation: High.
Line managers should check that their staff have completed all necessary mandatory training, including data protection and information security training and this should be monitored as part of the annual appraisal process.

Management response: Rejected
If PDR's were based on all training staff have to undergo, particularly in FS, there would be little else left.

Follow-up

b42. Although the data protection and information security policies confirm Line Managers are responsible for ensuring staff complete their training prior to access to the network and information systems, there are no mechanisms in place to ensure this happens in practice. It was reported that there have been incidences of Line Managers requesting staff have access to systems via IT before training has been completed.

Priority Recommendation: Urgent.
Responsibility for the identification and follow up of non-attendance at data protection and information security training should be clearly allocated. Line Managers should be reminded of their responsibility to ensure that their staff have received their training before they are granted access to systems as per the Information Security policy. Training completion statistics should be reported to the appropriate person/forum.

Management response: Accepted

Owner: HOIM/Line Managers
Date for implementation: December 2017

b43. Within Forensics Services, if a staff member fails to complete any of the required training including data protection and information security, the Line Manager would follow that up with the member of staff. If the staff member still does not complete the training it would be escalated to the Operations manager, then head of Function and finally the Director of forensics. Failure to complete all relevant training is a breach of the Code of Conduct and would result in disciplinary action.

Priority Recommendation: Medium.
Create a procedure for following up non-completion of data protection and information security training across SPA, clearly allocating responsibility for training follow up as appropriate. This process should be consistent across the organisation and reported centrally.

Management response: Partially Accepted
We will be ensuring that all SPA staff are aware of our role in training and we will be reporting on training to the relevant management group.

Owner: HOIM
Date for implementation: January 2018

b44. No similar process was reported for the rest of SPA. Non-attendance/non completion of data protection and information security training is not consistently followed up across the organisation.

8.3 Scope C: Data Sharing– The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

Risk: The failure to design and operate appropriate data sharing controls is likely to contravene the principles of the Data Protection Act 1998, which may result in regulatory action, reputational damage to the organisation and damage or distress for those individuals who are the subject of the data.

Recommendations	
Urgent:	6
High Priority:	15
Medium Priority:	1
Low Priority:	0

Informed Decision Making

c1. SPA policies, procedures and guidance do not include who makes decisions about sharing personal data and when it is appropriate to do so. The SPA Data Protection Policy makes reference to Information Sharing Protocols in relation to Data Processing agreements, but does not give any further guidance on systematic sharing or one-off disclosures with separate data controllers.

Priority Recommendation: High.
Create an information sharing policy that clearly sets out who has the authority to make decisions about systematic sharing or one-off disclosures, and when it is appropriate to do so. This should include general principles to consider when sharing SPA information and the roles and responsibilities assigned within the organisation for information sharing. Also include a template DSA and guidance for completing DSAs.

As part of the review and monitoring of compliance with this policy, SPA should conduct dip samples to ensure sharing is proportionate to the purpose and decisions are being recorded by following the audit trail from request through to disclosure. See the ICO Data Sharing Code of Practice and Data Sharing Checklists for further guidance.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

c2. SPA regularly share information with third parties such as Police Service of Scotland (PSoS), the Crown Office and Procurator Fiscal Service (COPFS) and the

Police Investigations and Review Commissioner (PIRC). SPA do not have formal Data Sharing Agreements (DSAs) in place with any of these separate agencies.

Priority Recommendation: Urgent.
SPA should identify all agencies with which they regularly share information. Formal data sharing agreements should be established as a matter of urgency. These agreements should:

- set out common rules to be followed by all partners in the sharing be signed off by a senior staff member, for example the CEO;

- specify how long shared data is to be retained for before it is to be returned to the data controller or securely destroyed;

- specify security arrangements relating to the transfer of shared data and access to shared data; and

- be subject to regular review to ensure partner organisations are removed from or added to agreements when required, and to regularly examine the working of the agreement.

Management response: Rejected
SPA does not believe that information sharing protocols are required where the law prescribes that SPA must make disclosures, as in the case of the organisations highlighted. SPA believes that we are primarily a data processor and PSoS acts as our agent for the data where we are a data controller so we think they would manage the DSA. Of course, the important thing would be to recognise if this changes and put in relevant processes and procedures at that point.

ICO comment
We note the rejection of this and numerous other data sharing recommendations. We have serious concerns about SPA's obvious confusion, misunderstanding and lack of awareness of how the data protection act applies to the sharing of personal data and their legal obligations and responsibilities as a data controller.

The data sharing code of practice is a statutory code which has been issued after being approved by the Secretary of State and laid before Parliament. We strongly advise SPA to urgently review and reconsider their management responses to the rejected recommendations for this scope area.

c3. SPA have a DSA in place with the Scottish Police Recreation Association (SPRA) and PSoS in relation to the provision of payroll information to SPRA. This was written by the HoIM and signed off by the CEO. This is the only DSA in place between SPA and other agencies with which they regularly share information.

c4. SPA do not formally document all sharing decisions for audit, monitoring and investigation purposes.

Priority Recommendation: High.
All sharing decisions should be recorded (i.e. reasons, purpose, decision making process and rationale) providing a complete audit trail should the decision to share or not to share be challenged.

Management response: Rejected

ICO comment
Please refer to ICO comment at **c2**.

c5. Generic data protection training includes information on disclosures however this is potentially confusing for staff. One slide advises that the IMT are responsible for advising on disclosures whereas another tells staff to get requests in writing and consider whether the disclosure is in line with SPA's purposes. There is a risk that staff are processing third party requests for information without the involvement of IMT. Auditors were told that SPA intends to amend the training to state that only IMT should deal with requests for information.

Priority Recommendation: High.
SPA should ensure that staff are adequately trained in recognising requests for information and responding appropriately, for example, by directing all requests to the Information Management Team. SPA should ensure generic and role-based training needs are identified and met on appointment and, where appropriate, periodically thereafter.

Please refer to recommendation at **b10** regarding training needs analysis.

Management response: Accepted

Owner: HOIM
Date for implementation: January 2018

Fair Processing Information

c6. SPA do not provide data subjects with fair processing information or seek consent to share information with third parties where necessary. For example, standard responses to complaints do not contain information such as who their information will be shared with, for what purpose or for how long it will be retained.

Priority Recommendation: Urgent.
SPA should make fair processing information about sharing and the purpose shared readily available to data subjects, unless an exemption applies, for example via the SPA website. Where necessary, fair processing information should

be actively communicated to individuals and their consent to share information with third parties sought. Further information about privacy notices under the GDPR is available on the ICO website.

Management response: Accepted

Owner: HOIM/Head of Complaints
Date for implementation: November 2017

Assessing legality, risks and benefits (PIA)

c7. The SPA Data Protection Policy states that Privacy Impact Assessments (PIAs) must be completed in the event of 'new collection of data'. The Policy does not state that PIAs should be completed to make informed decisions about whether to proceed with sharing in a secure manner, minimising personal data and if anonymised data can be used instead. No PIAs have been completed since SPA was created.

Priority Recommendation: High.
Retrospective PIAs should be completed in relation to current data sharing. Include requirement in Information Sharing policy recommended at **c1.**
To ensure that sharing is fair and lawful, instances of sharing should be considered on a case by case basis and a clear justification of how such exchanges of data fulfil the requirements of the DPA recorded. In addition, where necessary, condition(s) for processing should be recorded.

Management response: Partially Accepted
Recommendation is rejected if it is related to c2. If it relates to the ad-hoc disclosures being made by FS then it is accepted. We have shut down all sharing (if there was indeed any) that isn't required by law, instructed by the data controller or done under defence access policy. We don't think there was any ad hoc disclosures. We were making disclosures, but only those that PSoS told us to make.

Owner: N/A
Date for implementation: N/A

ICO comment
Please refer to ICO comment at **c2.**

c8. SPA have not assessed and documented the legal basis for sharing information with third parties on an ongoing basis. It was reported that the legal basis for sharing would be considered in circumstances that were not 'routine' on a case-by-case basis.

Priority Recommendation: High.
SPA should assess and document the legal basis for regularly sharing information with third parties. This should form part of the PIA (see recommendation **c7**) and included in the DSA.

Management response: Partially Accepted
Not accepted for c2, but if its ad-hoc then accepted.

Owner: N/A
Date for implementation: N/A

ICO comment
Please refer to ICO comment at **c2**.

Information Sharing Agreements and logs

c9. As mentioned previously mentioned, SPA do not have DSAs in place with all partners with whom they regularly share personal data. Auditors were told that the requirement to have high level agreements setting out the common rules to be followed by all partners is in the SPA Data Protection Policy; however, the DP Policy does not include this requirement.

Priority Recommendation: Urgent.
See recommendation at **c2**. The requirement to have DSAs in place should be documented in policy. Relevant staff should be made aware of this requirement. Retrospective DSAs should be completed for current sharing agreements.

Management response: Rejected
As the only partners we regularly share personal data with are those highlighted in c2.

ICO comment
Please refer to ICO comment at **c2**.

c10. Auditors were informed that SPA had historically drafted a data processing agreement to formalise their data sharing relationship with PSoS. PSoS did not sign this agreement and instead produced a Memorandum of Understanding between the two parties. However, this was rejected by SPA and the status quo has remained.

Priority Recommendation: Urgent.
See **c2**. SPA should introduce a DSA with PSoS as a matter of urgency. Please refer to recommendation at **c9**.

Management response: Rejected
SPA believes that, as PSoS is a data processor for us it should be a data processing agreement and not a data sharing agreement. Police Scotland give us data to perform forensic analysis etc on, thus they give us personal data – as such I would have thought that it is for them to issue either a data processing agreement or a data sharing agreement. We do not give PSoS personal data they do not already own. If they didn't give us the personal data in the first place then we wouldn't hold it. As such it is PSoS that collect and ascertain the accuracy of the data before providing it to us for further examination.

ICO comment
Please refer to ICO comment at **c2**.

c11. As there are no formal DSAs in place or log of sharing activities, it is possible that currently SPA are not aware of all the sharing of personal data that takes place between themselves and third parties.

Priority Recommendation: Urgent.
SPA should ensure that all regular information sharing is documented and controlled through a DSA. SPA should take a proactive approach by sending a Data Sharing Survey to all business areas including Forensic Services to detail any information sharing they are involved in to identify gaps and enable the provision of advice and guidance with creating a formal DSA.
The completion of the data sharing survey task by all business areas should be mandated and tracked through the appropriate forum with regular reports on progress provided to the SIRO by the HoIM.

Management response: Accepted

Owner: HOIM
Date for implementation: December 2017

c12. SPA do not have statements of compliance signed by the senior management of each organisation involved in sharing, committing them to comply with the terms of agreement, as there are no agreements in place.

Priority Recommendation: High.
See **c2.** In addition to the agreements themselves, SPA should have statements of compliance signed by senior management of each party involved in the sharing. SPA should conduct regular compliance checks with sharing partners to ensure the terms of the agreement and framework is being adhered to and any issues raised should be reported to the appropriate forum/SIRO.

Management response: Accepted

Owner: HOIM
Date for implementation: Tbc

c13. SPA does not have a review process in place to ensure that DSAs remain up to date and fit for purpose.

Priority Recommendation: High.
Once DSAs are completed and authorised by the HoIM/SIRO introduce a review process to ensure partner organisations are removed from or added to agreements when required, and to regularly examine the working of the agreement. See **c2**.

Management response: Rejected
We think it's unlikely we will have DSA's as in the new Act we are going to be a data processor and PSoS discharge our functions in respect of our other data controller duties and as such they should have data sharing agreements.

ICO Comment
Please refer to ICO comment at **c2**.

c14. There is only one DSA in place which is stored in a folder.

Priority Recommendation: High.
See **C2**. Once DSAs are in place, these should be centrally logged to ensure oversight of agreements and that they are regularly reviewed and kept up to date.

Management response: Accepted
When/if the first new DSA is completed then the recommendation will have been discharged. We can't give a date as we don't have any agreements to log as yet.

Owner: HOIM
Date for implementation: Tbc

Data quality and retention

c15. It was reported by Forensic Services that they would not redact or minimise shared data as it is created for a particular purpose with the intention of being shared with a third party. Auditors were told that shared information is factual so it would not be necessary for SPA to distinguish between fact and opinion.

c16. SPA does not have processes in place to ensure that shared data is kept accurate and up to date, for example through regular quality checks or verification

by data subjects. The DP Policy states that where inaccurate data has been shared with a third party, the third party should be notified within two working days. SPA were unable to provide specific examples of this occurring in practice.

Priority Recommendation: High.
SPA should implement formal processes to ensure that shared data is kept accurate and up to date. Ensure staff who are actively sharing data with other agencies are conducting data quality checks on the information prior to sharing and if appropriate inform recipients when any amendments or updates are made.

Management response: Rejected

ICO Comment
Please refer to ICO comment at **c2**.

c17. SPA use the PSoS retention schedule and it was reported that they have previously requested amendments or additions to this schedule. SPA trust that PSoS will delete shared information in line with this retention schedule; they do not seek any assurances that shared data has been deleted or securely destroyed once the relevant retention period has expired.

Priority Recommendation: High.
SPA should ensure the storage and destruction of the data is aligned with their own retention and disposal policy/schedule and details the specific arrangements in each DSA.

Management response: Rejected

Information Sharing Security

c18. SPA use the Government Protective Marking Scheme (GPMS) to classify information and apply security measures as appropriate. Auditors were informed that SPA will move over to the newer Government Security Classification (GSC) but did not have a timeframe for this, as this is controlled by PSoS.

Priority Recommendation: High
SPA should ensure all agreements specify the protective marking to be applied to the data before being shared. This will ensure a level of sensitivity is understood particularly if different organisations have different standards.

Management response: Accepted
We already mark everything using Titus, we are dependent on PSoS re moving to GSC and they have no date for doing so.

Owner: HOIM
Date for implementation: Tbc

c19. SPA does not have data sharing agreements in place with all external agencies with whom they share data. There is therefore no formal record of how data will be shared or restricted to authorised personnel within each organisation on the basis of business need.

Priority Recommendation: Urgent.
Please refer to recommendation at **c2**.

Management response: Rejected

ICO Comment
Please refer to ICO comment at **c2**.

c20. It was reported that SPA log potential security incidents involving shared data, for example if a third party requests a duplicate disk of information already provided by the SPA, they will presume this is because the original has been lost and log this as an incident. As there are no formal DSAs in place, there is no formal requirement for third parties to report actual or potential security incidents to SPA. There is no formal procedure for the reporting and investigation of incidents involving shared data.

Priority Recommendation: High.
Please refer to recommendation at **a82, a85** and **a90**. DSAs should include the requirement to report all actual and potential security incidents and 'near misses' to the Information Management team so that they can be investigated and resolved appropriately.

Management response: Rejected

Disclosures

c21. SPA frequently receive requests from third parties for one off disclosures, for example, Forensic Services often receive requests from solicitors and other third parties in relation to civil claims. SPA does not have an overarching policy or procedure on disclosures available for staff. Auditors were informed that Forensic Services follow their own policies and procedures but no evidence of this was provided.

Priority Recommendation: High.

SPA should devise a policy for all staff in relation to disclosures of personal data include requirements in the policy recommended at **c1**. This should include the steps that should be taken to verify the validity of the request, the requirement for disclosures to be recorded on Evidence Management System (EMS) and who is able to authorise one off disclosures to third parties.

Management response: Accepted

Owner: Director of Forensic Services
Date for implementation: January 2018

c22. It was reported that Forensics record on the EMS when disclosures are made to third parties and the basis for disclosure. Auditors were not provided with evidence that the legal basis for disclosure is recorded on EMS when information is provided to third parties.
Priority Recommendation: High.
SPA should ensure that all one off verbal or written disclosures to third parties are logged on EMS or other relevant system, including the legal basis for disclosure. Managers should conduct spot checks or compliance reviews. See **C1**.

Management response: Accepted

Owner: Director of Forensic Services/HOIM
Date for implementation: January 2018

Information Transfer

c23. SPA has guidance for staff relating to the acceptable use of communications facilities within the IS SOP and Electronic Communications SOP.

c24. The IS SOP includes procedures in relation to cryptography and states that staff should contact Information Management for guidance. All removable media such as CDs, DVDs and USBs is required to be encrypted according to policy. The Imaging Unit Working Processes document also states that removable media containing Images must be encrypted prior to sending them to a third party.

c25. SPA shares a retention schedule with PSoS. The IS SOP provides guidance in relation to the disposal of information, for example, information marked at PROTECT or above must be disposed of using a cross cutting shredder or via a third party accredited waste disposal provider.

c26. Email security is managed by PSoS as part of the provision of IT facilities; email applications have appropriate antivirus software. The Electronic

Communications SOP sets out the level of security that should be applied to emails depending on the protective marking, for example, information marked RESTRICTED may only be sent to secure email addresses such as those on the Police National Network. The Imaging Unit Working Processes document provided as evidence is in line with this procedure, for example, emails containing Images may only be sent via secure email.

c27. In the event of a member of SPA staff sending an email in breach of this, auditors were informed that the PSoS Information Security Officer would deal with the member of SPA staff directly. It was unclear whether PSoS informed the SPA IM of any such breaches of policy.

Priority Recommendation: High.
As Data Controller, SPA should ensure they have central oversight/governance of security incident management and follow up with all business areas. This will ensure all incidents involving personal data are satisfactorily resolved and that lessons learned are communicated to staff. In addition any risks identified during investigations can be monitored and mitigated against by the HoIM/SIRO consistently on an ongoing basis.

Management response: Accepted

Owner: PSoS
Date for implementation: Tbc

ICO Comment
SPA did not provide the ICO with any indication of acceptance of recommendation or data for implementation.

c28. SPA use 7zip encryption to password protect email attachments above GPMS marking PROTECT. This requirement is documented in the Electronic Communications SOP. It was unclear if any spot checks or reviews are undertaken to assess staff compliance with this requirement.

c29. Interviewees reported that they would provide hard copy information to third parties. The Imaging Unit Working Process is for hard copy photographs to be provided in line with evidence production procedures, e.g. in a sealed evidence bag. The IS SOP does not include physical transfer procedures. It was unclear what formal physical transfer procedures are in place for staff working outside of the Imaging Unit.

Priority Recommendation: Medium.
SPA should monitor compliance with these policies.

Management response: Rejected
The only physical transfer of data that occurs is in FS and we have a secure, accredited, provider that moves hard copy or evidence. SPA at PQ doesn't move physical assets. The Protective Marking policy details how data in transit must be protected but does not specify the details of the FS data transit - are you asking that the IS sop references the FS process for moving assets around the country? If so it would be a link rather than detail, should the contract change.

8.4 The agreed actions will be subject to follow up to establish whether they have been implemented.

8.5 Any queries regarding this report should be directed to Liam Duncan, Group Manager, ICO Assurance.

8.6 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Lindsey Davie – Head of Information Management
Carol-Anne Hilley – Records Manager

ICO Data Protection Audit - Action Plan

Data Controller	Scottish Police Authority
Report Date	Apr-18

Scope Area	GDPR	Finding No	Priority	Recommendation	Accepted / Partially Accepted / Rejected	Agreed Action	Implementation Date	Owner
Security of Personal Data		a4	Low	Ensure the HoLC's job description is updated to reflect new role and responsibilities of acting SIRO.	Rejected	Job descriptions are not updated for 'acting' roles		
Security of Personal Data		a7	High	Review the current IS SOP to clearly define and outline responsibilities of key information security roles within SPA. The IS SOP should make reference to the roles and responsibilities of the SIRO, HoIM, RM and IAOs. Finding where there was an uncontrolled or poorly controlled risk that will require a recommendation to improve practices.	Accepted	Policy updated to reflect changes. Minor changes so no need for SMT approval	End October 2017	Head of IM
Security of Personal Data	GDPR 2.4	a8	Urgent	Where a third party (PSoS) is providing SPA with an ICT Service, the relationship and processing should be formally documented in a written contract. The supplier relationship agreement should include clear instructions to the ICT service provider defining what they can or cannot do with the data. The written contract should require the ICT service provider to act on SPA's instructions only. Please see recommendation at a83, in the 'Supplier Relationships' section.	Accepted	SPA have sought permission to engage a specialist lawyer to manage this issue with Police Scotland. This is part of the bigger overall issue of the data controller/data processor relationship that needs to be resolved prior to GDPR.	May-18	Director of Governance and Assurance
Security of Personal Data		a9	High	Review the current Risk Management Policy to ensure the policy outlines SPA's approach to information risk management. To ensure the content remains accurate and fit for purpose, ensure the policy is reviewed on annual basis.	Rejected			
Security of Personal Data		a11	Urgent	Ensure the corporate risk register includes SPA's information risks. Alternatively, create a separate information risk register. Similar to the current corporate risk register, the register should record a description of the risk, mitigating plan, rating and risk owner. The HoIM should be consulted in relation to all information risks to ensure all risks are effectively managed and mitigated.	Accepted	Information Management risks will be included within the SPA Corporate Risk Register. Any member of staff can propose risks to be added to the corporate risk register. New risks are reported to the Senior Management Group to approve inclusion in the risk register and also reported to SPA Audit Committee for noting. The HoIM will liaise with the risk and policy specialist to highlight relevant risks, taking cognisance of the audit findings, for inclusion in the corporate risk register. Since the audit was completed a risk has been added to the corporate risk register relating to GDPR.	In place	Director of Strategy and Performance
Security of Personal Data		a12	Urgent	Ensure the local risk register maintained by Forensic Services includes information risks. Please refer to recommendation at a11.	Partially Accepted		Jan-18	Director of Forensic Services

Security of Personal Data	GDPR 5.5	a15	Urgent	Create a PIA policy which sets out the requirement to conduct PIAs on all new projects, or changes to current processes that involve personal data to assess and identify information security risks. The PIA Policy should require project leads to conduct a PIA at the beginning of the project or change, to identify information risks and controls to mitigate those risks. Requiring a PIA to be conducted for projects and changes to existing systems will assist with the changes that are required to be implemented when GDPR is implemented in May 2018	Accepted		Nov-18	Head of IM
Security of Personal Data	GDPR 3.1 & 8.2	a16	Medium	To ensure there is an appropriate representative to discuss and report key information security issues to the Committee, ensure arrangements are made for the acting SIRO to attend quarterly meetings.	Accepted		Complete by 1st Quarter 2018	Director of Governance and Assurance
Security of Personal Data	GDPR 3.1	a17	High	Introduce a regular forum or steering group to discuss and report information security issues identified across the SPA. This group should be chaired by an appropriate senior level of staff i.e. SIRO and attendance should include key roles from departments across both corporate and forensic services. Attendance should include a member of PSoS IT service delivery team to report on IT related concerns.	Accepted		Nov-17	Director of Governance and Assurance
Security of Personal Data	GDPR 8.2	a18	High	Identify an appropriate role to attend the PSoS IT working group to ensure SPA has oversight of key issues and concerns discussed.	Accepted		Will be in place for next scheduled meeting in 2018	CEO
Security of Personal Data		a22	Low	Ensure all policies consistently incorporate the annual cycle of and responsibility for review, the next scheduled date for review.	Accepted		Jan-18	Head of IM
Security of Personal Data		a23	High	Policies and SOPs that apply to both SPA and PSoS should be reviewed by the IMT to ensure the content is fit, for purpose, consistent and align with SPA's policies and SOPs.	Accepted	This is part of ongoing dialogue between PSoS and SPA HR, i.e. that policy and procedure has been dual branded, but there has been no consultation with SPA in terms of content.	Apr-18	PSoS
Security of Personal Data		a24	Medium	Please see recommendation at a23. To ensure departmental policies and SOPs are consistent with corporate SPA policies, ensure IM is actively involved in the creation and review of SOPs relating to information security and management.	Accepted	FS will provide relevant SOPS to IM without delay, however, IM only has limited resources to review the policies	Jan-18	Director of Forensic Services
Security of Personal Data		a25	Medium	To ensure all SPA staff are aware of their information security responsibilities, relevant dual branded PSoS policies and SOPs should be identified and made available on the SPAs intranet webpage.	Rejected	Duplication could lead to out of date documents being circulated. The current system whereby links are provided will be maintained.		
Security of Personal Data		a26	Low	To prevent the risk of staff within Forensic Services referring to outdated information security and data protection related policies and SOPs, ensure a direct link to the to corporate policies and SOPs is provided.	Rejected	The ICO staff misunderstood what FS staff were explaining. SOPs are not stored separately on FS domain, there is a link to the Intranet from Q pulse, so the risk highlighted does not exist		
Security of Personal Data	GDPR 6.6	a27	High	Ensure induction checklists include the key information security policies and SOPs that new starters are expected to read, in order to facilitate compliance. To ensure staff are aware of, and agree to, their information security obligations and responsibilities mandate that all permanent, temporary and contract staff, sign an agreement to confirm that they have read and understood all information security related policies and SOPs.	Accepted	FS will work with the HOIM to explore the use of Q pulse whether this could be extended across the organisation	Nov-18	Head of IM
Security of Personal Data		a28	High	Ensure policies and SOPs created are reviewed and formally approved by senior management. Once a process has been agreed for policy approval, create a procedure which outlines the agreed process to staff. Timeframes in which policies or SOPs should be signed off should be defined to ensure policies are promptly approved, implemented and disseminated to staff.	Accepted	Update Dec 18: Senior Management Group will now approve policies	May-18	CEO/IM
Security of Personal Data		a32	High	Enforce regular password changes as needed for remote devices.	Rejected	The ICO staff misunderstood this. Password changes are enforced.		
Security of Personal Data	GDPR 6.6	a35	High	Create a mobile device asset register which records all mobile devices in use by SPA.	Accepted	This action is dependent on PSoS compiling an asset register, which they don't currently have.	Mar-18	PSoS

Security of Personal Data	GDPR 6.6	a36	High	Training should be implemented for personnel using mobile devices to ensure they are aware of their responsibilities when using devices, and to raise awareness of the additional security risks resulting from remote working and the security controls that should be implemented. Once trained and prior to issuing mobile devices to personnel, ensure users have signed a user agreement acknowledging their duties and responsibilities when using mobile devices.	Accepted	SPA IM do not always know who has been allocated such devices. However, once a35 has been completed the users will be provided with training. PSoS ICT will need to agree that all requests for mobile assets, including phones, comes through SPA IM (as it should) and refrain from the current process where they take verbal requests for jobs from senior staff.	Jan-18	Head of IM
Security of Personal Data	GDPR 6.1	a37	High	Undertake regular security spot checks to ensure the security of mobile devices and compliance with the Remote Working Policy.	Accepted	As per a35, spot checks will commence after we create register. SPA has been unable to do this due to the lack of asset register held by ICT. Each business area will assign an auditor to conduct spot checks and send reports back to HOIM.	01/03/2018	Head of IM
Security of Personal Data	GDPR 1.6	a39	High	Create an IAR which identifies and records all information assets (both electronic and physical) held by SPA and their importance. The IAR should include information assets held by SPA PQ and Forensic Services and include the creation, processing, storage, transmission, deletion and destruction of the asset and should be continually risk assessed to ensure information assets are kept secure. Once created, the IAR should be subject to regular review to ensure it is accurate, up to date and consistent. This can be achieved by adopting a similar method and conduct data reviews of all departments within SPA.	Accepted		Work will commence November 2017	Head of IM
Security of Personal Data		a41	High	Ownership for all physical and electronic information assets identified should be assigned. IAOs assigned should be recorded on the corporate IAR. Roles and responsibilities of an IAO should be formally documented in job descriptions.	Accepted		Dec-17	Head of IM/HR
Security of Personal Data	GDPR 5.6	a42	High	To prevent unauthorised disclosure, modification, removal or destruction of personal information stored on media, review and update the current Remote Working Policy to include guidance on the use and management of removable media, including the restrictions on the import and export of personal data via the media. Disseminate the updated policy to all staff.	Accepted		Dec-17	Head of IM
Security of Personal Data	GDPR 6.6	a44	Low	Please refer to recommendation at a36 regarding the requirement for staff to sign a user agreement for the use of mobile device.	Accepted		Dec-17	Head of IM
Security of Personal Data	GDPR 6.6	a46	High	Ensure a USB log is maintained which documents the USB devices used by SPA, the location they have delivered to, the name of the individual who has been allocated the USB and date returned where appropriate.	Accepted		Nov-17	Head of IM
Security of Personal Data	GDPR 6.7	a49	High	To prevent unauthorised access to data held on SD cards, ensure new, up to date SD cards are used. All data on SD cards should be wiped and securely destroyed to prevent the data from being recoverable.	Accepted		Dec-17	Head of Scene Examination
Security of Personal Data	GDPR 5.2	a50	High	Create an Access Control Policy or SOP which provides clear guidance to Line Management and staff regarding the processes to follow when requesting ICT user access or physical access to the building for new starters. For staff that change roles or leave SPA employment, the policy or SOP should include procedures for amending or removing unnecessary access permissions to the network and individual systems/applications and physical access to buildings to help ensure that staff are only able to access information on a 'need to know' basis and access is removed in a timely fashion. Once created the Policy or SOP should be regularly reviewed.	Accepted		Dec-17	Records Manager
Security of Personal Data	GDPR 5.2	a51	High	Please refer to recommendation at a50. Ensure the Access Control Policy or SOP includes the requirement for HR to notify the new starter's Line Manager once their vetting has been completed to enable the Line Manager to proceed with requesting an account to be setup.	Accepted		Dec-17	Records Manager

Security of Personal Data	GDPR 5.2	a54	High	To control user access and to ensure users are only provided with access to networks and systems that are relevant to their specific job role. IAOs/system owners should determine which job roles that require access to the information systems/assets they are responsible for. This should be formally documented and kept under review.	Accepted		Dec-17	Records Manager
Security of Personal Data	GDPR 5.2 & 6.7	a55	High	Ensure the leavers and movers procedure documented within the Access Control Policy or SOP sets out the requirement for Line Managers to notify HR of any leavers or movers within the department. Please refer to recommendation at a50.	Accepted		Dec-17	Records Manager
Security of Personal Data	GDPR 5.2 & 6.6/7	a56	High	Please refer to recommendation at a51 and a52 to ensure controls are in place to improve communication between departments.	Accepted		Dec-17	Records Manager
Security of Personal Data	GDPR 5.2 & 6.6/7	a57	High	In addition to the policy or SOP recommended at a50, create a new starter/movers/leavers checklist, which provides guidance to Line Managers on the steps that should be taken in the event of a staff member joining, moving or leaving the department. This should include the requirement to notify HR and ICT.	Accepted		Dec-17	Records Manager
Security of Personal Data	GDPR 6.2	a58	Urgent	Ensure regular proactive monitoring of information systems access through random dip samples of access attempts. Access rights should be audited regularly to ensure that individuals with no right of access to specific systems or applications are removed.	Accepted		Q1 2018	Records Manager to identify department leads. FS to identify their leads
Security of Personal Data		a60	Urgent	To ensure the protection of protectively marked information assets, ensure regular physical security risk assessments are carried out by the IMT. Assessments should include physical access to building, passes, reception area, visitor's procedures, location of equipment that can access criminal databases, locks on offices or areas processing personal data, shared office area and vetting levels of staff. Physical security assessments should be formally documented for audit and monitoring purposes. Recommendations as a result of assessment should be followed up to ensure appropriate controls have been implemented.	Rejected	ICO comment: SPA has challenged the accuracy of this finding and have claimed that physical security risk assessments are carried out; however, no evidence was provided to Auditors to support that assertion.		
Security of Personal Data		a61	Urgent	Please refer to recommendation at a60.	Rejected	See a60		
Security of Personal Data	GDPR 6.3	a68	High	Proactively conduct physical access control audits to ensure staff only have access to the permitted areas of the building. Conducting regular physical access control audits will also assist SPA with identifying staff that are still registered to have access to the building but have left the organisation.	Accepted		Nov-17	Head of IM
Security of Personal Data	GDPR 6.1	a69	Urgent	Ensure the clear desk and screen procedures are communicated to all staff and any relevant third party contractors and home/remote workers. Line Managers and the IMT should carry out spot checks at the end of the business day to ensure personal data has not been left unattended and staff adherence to the clear desk policy. Printers should be checked to make sure information is not left unattended during the day or overnight. Staff should also be told to lock their workstations using "ctrl-alt-delete" when not in use and monitor compliance. Spot checks should be formally documented for audit and monitoring purposes.	Accepted		Nov-17	IM / Line Managers
Security of Personal Data		a71	Urgent	Documents containing personal or sensitive personal data should be stored in a secure room, or a lockable filing cabinet or unit. Keys to offices or filing cabinets should be held in a secure key safe within the department. Access to information should be restricted on a need-to-know basis only.	Accepted		TBC	Records Manager
Security of Personal Data	GDPR 6.1	a72	Urgent	Please refer to recommendations at a69 and a71.	Accepted		Complete in terms of securing the files	Head of Legal
Security of Personal Data		a73	Urgent	Please refer to recommendation at a69 regarding reinforcing clear desk policy. Review the current guidance in the Handbook regarding password complexity rules to include password rules regarding the management of passwords.	Accepted		Nov-17	Head of IM
Security of Personal Data	GDPR 6.7	a74	High	Ensure all end of life IT equipment is collected and securely destroyed. The Asset register should be updated accordingly to record the destruction of old equipment.	Partially Accepted	IM staff will now put on ICT requests to have kit collected, however, the update of the central asset register after destruction is a matter for PSoS, not SPA.	Implemented	Head of IM / ICT
Security of Personal Data	GDPR 6.7	a75	High	Where a third party is used to dispose of confidential waste, ensure certificates of destruction are obtained to gain assurance that confidential waste has been securely destroyed.	Accepted		01/12/2017	Head of IM

Security of Personal Data	GDPR 6.7	a80	Urgent	Please refer to recommendation at a69.	Partially Accepted	Spot checks are conducted, however, it is accepted that from time to time there are some documents appearing. This has been taken on board and checks will be conducted more frequently and reminders issued regularly		Director of Forensic Services
Security of Personal Data		a81	Urgent	Please refer to recommendation at a71.	Accepted	A review of storage is already underway as it is accepted that more storage is needed for when files are recalled from storage. Key boxes in situ and temporary storage freed up in the interim.	Complete	Director of Forensic Services
Security of Personal Data	GDPR 2.4 & 5.3	a82	Urgent	Please refer to recommendation at a8, within 'Information Security – Organisation' regarding the creation of a written contract. Information security requirements should be established and agreed with PSoS within the written agreement. The following terms should be included for inclusion within the contract to address information security requirements; description of data accessible, legal and regulatory requirements (DPA), obligation by PSoS to implement an agreed set of access, monitoring and reporting controls, rules of acceptable use of information, explicit list of supplier personnel authorised to access SPA information, incident management, training and awareness and right to audit.	Accepted	Agreed as part of the whole agreement that needs to be documented with PSoS with the temporary legal resource that we are hiring	Apr-18	Director of Governance and Assurance
Security of Personal Data	GDPR 5.3	a85	Urgent	An Information Security Management Policy or SOP for supplier relationships should be created. This should identify information security controls to address supplier access to information (Please refer to recommendation at a83 regarding controls that should be included). The processes and procedures to be taken when entering into an agreement should be set out. Creation of a policy or SOP would ensure a consistent approach is adopted throughout SPA when entering into a supplier agreement.	Accepted	ICO comment SPA were unable to provide the ICO with an indication of the date by which this recommendation is to be implemented and what steps will be taken to ensure compliance due to a lack of response from the PSoS.	No date	PSoS
Security of Personal Data	GDPR 5.3	a87	Urgent	To ensure SPA has oversight of all ITT, ensure the HoIM at SPA is involved in the ITT process and drafting of supplier contracts to review to ensure all information security requirements have been addressed and included in the contract.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS / Director of Governance
Security of Personal Data	GDPR 5.3	a88	High	To ensure suppliers' staff are aware of their responsibilities when handling protectively marked information, require suppliers to deliver information security training to staff. Evidence of the delivery of training should be requested from suppliers to gain assurance.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Security of Personal Data	GDPR 5.3	a89	High	Where the third party supplier contract relates to the processing of SPA's personal data, ensure the written contract includes the requirement for the third party to report all information security incidents to the HoIM at SPA. The contract should include clear instructions for the third party supplier to follow when reporting a breach. Contact details of SPA's HoIM should be included within the contract.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Security of Personal Data	GDPR 5.3	a90	Urgent	Please refer to recommendation at a85 regarding the creation of an Information Security Management Policy or SOP for Supplier relationships and a87 regarding SPA oversight of all supplier relationship agreements.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Security of Personal Data	GDPR 5.3	a91	High	Ensure that the contracts include the right for SPA to conduct regular audits. Conduct regular supplier audits to ensure compliance with the security requirements set out within the contract. Audits should be formally documented for monitoring purposes.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Security of Personal Data	GDPR 5.4	a93	High	Develop an Information Security Incident Management Policy, setting out roles and responsibilities for managing information security incidents, detailing how to identify and report an incident, and signposting where to seek further guidance. Publicise the policy to ensure staff awareness of their information security incident management responsibilities. Consider creating an incident reporting form on SPA's intranet that staff can use to report information security incidents.	Accepted	Blank	Dec-17	Head of IM

Security of Personal Data	GDPR 3.2 & 5.4	a94	High	Please refer to recommendation at a97.	Accepted	Blank	Dec-17	Head of IM
Security of Personal Data	GDPR 3.2 & 5.4	a95	High	Create a procedure for all business areas within SPA to formally record and report information security incidents identified centrally to IMT. Centralising the reporting mechanism would ensure all information security incident are effectively reported, logged and management by IMT to prevent further incidents. The procedure should be included in the Information Security Incident Policy recommended at a95.	Accepted	Blank	Dec-17	Head of IM
Security of Personal Data	GDPR 3.2 & 5.4	a97	High	A procedure which provides guidelines to staff responsible for investigating security incidents should be created. The document should include the process to follow once a security incident report has been received, risk assessing the potential harm and distress, logging and circumstances in which security incidents may need escalating or reporting to external bodies e.g. ICO.	Accepted	Blank	Dec-17	Head of IM
Security of Personal Data	GDPR 3.2	a98	High	Please see recommendation at a93 and a95 regarding the creation of a formal procedure which is included in the recommended Information Security Incident Management Policy to centralise reporting from all business areas including PSoS to IMT.	Accepted	Blank	Dec-17	Head of IM
Security of Personal Data	GDPR 3.2	a100	High	Lessons learned from analysing and resolving a security incident should be communicated to staff to reduce the likelihood or impact of future security incidents.	Partially Accepted	The lessons learned are not always relevant for dissemination to staff.	As Required	Head of IM
Security of Personal Data	GDPR 3.2	a101	High	To ensure senior management within SPA have appropriate oversight, ensure both cyber and physical related information security incidents are reported to the Committee. Reports should explain the security incidents occurred within the quarter, the severity of the incidents, action taken to resolve/mitigate the incident and escalation.	Accepted	Blank	Jan-18	CEO/Audit Committee
Security of Personal Data	GDPR 6.3	a103	High	SPA should conduct regular information security audits to assess compliance with relevant policies and procedures. Audit reviews should ensure the continuing suitability, adequacy and effectiveness of SPA's current approach to information security.	Accepted	We were just getting agreement on resources for this. We are going to use our external auditors.	Apr-18	CEO/Audit Committee
Security of Personal Data		a104	High	Create an action plan and ensure that the recommendations from the IT Health Check are implemented. Please also refer to recommendation at a8.	Accepted	Blank	No date	PSoS
Security of Personal Data		a107	High	Create a programme of spot checks and/or staff surveys to assess and promote compliance with SPA's information security policies and procedures.	Accepted	This duplicates earlier recommendations where single areas where pulled out, such as clear desk, could have been one recommendation	1st Quarter 2018	Head of IM / Records Manager
Security of Personal Data	GDPR 2.4 & 5.3	a108	High	Please refer to recommendation at a8 and a82 regarding the requirement to formalise the services provided to SPA to ensure oversight.	Accepted	Blank	No date	PSoS
Training & Awareness	GDPR 8.2	b1	High	A management framework should be put in place with a delegated process of accountability and responsibility from the board down, to ensure the effective oversight of data protection and information security training.	Accepted	Blank	1st Quarter 2018	Chair of Board / CEO
Training & Awareness	GDPR 3.1	b2	Urgent	Create an Information Management steering group to monitor and mandate data protection and information security training and improvements. This group should be chaired by the SIRO and include the Head of Information Management. The Steering Group should report to the Board.	Accepted	The SIRO and HOIM support this recommendation and have discussed group membership with agreement from general business areas, however, the Board need to agree re the reporting mechanism. It is felt that, given the size of SPA that b2 and a17 could be one Group that will then report to the CEO who will report to the Board.	Feb-18	Director of Governance and Assurance / Chair of Board
Training & Awareness	GDPR 8.7	b3	High	Responsibility for DP and IS training should be allocated to an appropriate individual who will be responsible for training across the entire organisation. That person should be key in the development and implementation of the TNA and training plan.	Partially Accepted	FS will allocate resources to perform a TNA and will assist the IMT to ensure that where they deliver training to FS staff, records are updated accordingly.	1st Quarter 2018	Head of IM / Director of Forensic Services

Training & Awareness	GDPR 8.7	b4	Medium	Ensure the Overall responsibility for data protection and information security training is recorded in the relevant policies and corporate training plans.	Accepted	The job descriptions are all being changed in February 2018 as a result of job evaluation.	No date	Head of IM
Training & Awareness		b8	High	Ensure all departmental data protection training is provided by the IMT to ensure consistency across departments.	Rejected	This was rejected at the time, however, issues with GDPR training have highlighted that there are issues with IM not being the central point for IM training		Head of IM
Training & Awareness	GDPR 8.7	b9	High	A data protection and information security training programme should be developed across the whole of SPA and should include Forensic Services. This should be approved by senior management and mandated for all staff.	Accepted	SPA comment CEO has now approved scoping an e-product. We would like to develop and implement a full suite of e-training. However, we will increase face-to-face and intranet bulletins in the interim.	2nd Q 2018	Head of IM
Training & Awareness	GDPR 8.7	b10	Urgent	SPA needs to ensure that a Training needs analysis is completed for all staff including temporary and contract staff. This should be based on the staff member's job role and how much access to personal data they have. This will help the understanding of what training needs to be provided to staff in each department of SPA.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Training & Awareness	GDPR 8.7	b11	High	SPA needs to develop a training plan or strategy to meet training needs within agreed timescales.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Training & Awareness	GDPR 8.8	b12	High	Document within the organisations Data Protection policy when staff members are required to complete mandatory data protection and information security training and monitor compliance.	Accepted	Blank	Dec-17	Head of IM
Training & Awareness		b14	High	Induction checklists should be submitted centrally so Information Management have oversight of its effectiveness.	Rejected			
Training & Awareness	GDPR 6.6	b15	High	Ensure that all staff receives a copy of the Information Assurance Handbook at induction. Staff should sign acknowledgement of this and this should be recorded on their scope record.	Partially Accepted	The Handbook was intended as an aide memoir, not an official document. However, a checklist will be drawn up for staff to sign at induction to record their agreement that they have been informed of the key relevant policy/procedure and understand that it is their responsibility to read the policy. This checklist could include 'provided with Handbook'. Need to establish how this can be recorded on Scope	No date	Head of IM
Training & Awareness	GDPR 6.6	b16	Medium	SPA should ensure that all attendees sign to confirm that they have completed induction training. The attendance record should be retained and logged on a staff member's Scope record to ensure that training is delivered to all staff including temporary contract and senior staff.	Accepted	Need to engage with HR in terms of updating scope records. FS will manage theirs locally if IM provide data.	1st Quarter 2018	Head of IM
Training & Awareness	GDPR 8.2	b18	High	Employees at all levels including senior managers need to be aware of what their roles and responsibilities are, specifically in relation to data protection, information security and their employment at SPA. Ensure this training is mandated for all staff and senior managers should lead by example.				
Training & Awareness	GDPR 6.6	b19	Medium	SPA should review and update the content of induction training on an annual basis to ensure that it remains relevant and up to date. This is especially important in light of the new GDPR legislation.	Accepted	Blank	Apr-17	Head of IM
Training & Awareness	GDPR 6.6	b20	High	Develop a test for the end of the data protection induction training. It should have a minimum pass mark of at least 70% to provide SPA with assurances that staff have understood the content of the presentation.	Accepted	Blank	2nd Q 2018	Head of IM
Training & Awareness	GDPR 8.8	b21	Urgent	To ensure staff are up-to-date with current legislation and also with organisational developments regarding data protection and information security it is recommended that SPA introduce regular mandatory refresher training for all staff, including temporary and contract staff, at all grades. This is particularly relevant for staff who have regular access to personal data. This will help to ensure staff remain aware of their data protection obligations and responsibilities.	Accepted	Blank	In line with all training recommendations that have dependencies	Head of IM
Training & Awareness	GDPR 8.8	b22	High	Refresher training sessions should be delivered to all staff on a regular basis. The contents of any refresher training should be approved at an appropriate level and delivered to all relevant staff including temporary and contract staff. Refresher training can be bespoke and relevant to individual teams.	Accepted		As per 21	Head of IM

Training & Awareness	GDPR 6.6	b23	High	SPA should develop a starter, movers and leavers process to ensure that their records are accurate and up to date and that only relevant staff are provided access to SPA information and systems.	Accepted	ICO comment Please refer to ICO comment at a85.	No date	PSoS
Training & Awareness	GDPR 8.7	b24	Medium	SPA should grant access to Moodle across the entire organisation to ensure the same level of training is accessible for all staff.	Accepted	Blank	Jan 17 (?) to include new DP legislation training	Head of IM
Training & Awareness	GDPR 8.7	b25, b26	High	SPA should ensure that all staff that require specialised training are appropriately identified through a TNA and trained as necessary. SPA should also use or make reference to, relevant ICO statutory guidance/codes of practice, where appropriate.	Accepted	Blank	TBC	b25 - Head of IM b26 - CEO
Training & Awareness	GDPR 6.8 & 8.7	b27	Low	Develop a checklist to ensure a consistent approach when responding to requests.	Rejected		May-18	
Training & Awareness	GDPR 6.8 & 8.7	b28	High	Ensure staff are fully trained in recognising a request for information so that those requests are referred to the correct department and responded to within the statutory timeframe.	Accepted	Blank	May-18	Head of IM
Training & Awareness	GDPR 8.7	b31	Medium	Allow staff the opportunity to provide feedback on the induction training and refresher training to identify any key themes that can be incorporated into the training.	Accepted	Blank	May-18	Head of IM
Training & Awareness	GDPR 8.10	b32	Low	Improve the Information Management intranet page for staff to visit for advice. If not already available, staff should be able to find advice for a range of data protection issues, such as security, data incident management, SARs, information sharing, fair processing and exemptions.	Accepted	Blank	1st Quarter 2018	Head of IM/Corp Comms
Training & Awareness	GDPR 8.10	b33	Low	SPA should consider implementing the Q Pulse system or similar throughout its other departments to ensure staff have read new or amended policies and procedures.	Partially Accepted	The FS quality manager will look at the possibility of using Q Pulse across the estate	1st Quarter 2018	Director of Forensic Services / Head of IM
Training & Awareness		b37	Urgent	SPA should implement a mechanism to monitor staff completion of mandatory training. This will allow SPA to identify staff that need to complete induction or refresher training.	Rejected			
Training & Awareness		b38	High	SPA should ensure that training completion is accurately recorded on staff scope records and kept up to date.	Accepted	Blank	Dec-17	Line Managers
Training & Awareness		b39	High	Forensic Services training statistics should be regularly provided to Information Management to ensure that there is central oversight of data protection and information security training.	Rejected			
Training & Awareness		b40	High	KPIs should be agreed and statistics should be produced on a monthly basis in order to actively monitor SPA performance to training completion.	Rejected	SPA has a huge burden in terms of training, particularly in forensics. It would be completely unrealistic to have KPI's for all training		
Training & Awareness		b41	High	Line managers should check that their staff have completed all necessary mandatory training, including data protection and information security training and this should be monitored as part of the annual appraisal process.	Rejected	If PDR's were based on all training staff have to undergo, particularly in FS, there would be little else left		
Training & Awareness	GDPR 8.2	b42	Urgent	Responsibility for the identification and follow up of non-attendance at data protection and information security training should be clearly allocated. Line Managers should be reminded of their responsibility to ensure that their staff have received their training before they are granted access to systems as per the Information Security policy. Training completion statistics should be reported to the appropriate person/forum.	Accepted	This could form a single recommendation with b43	Dec-17	Head of IM / Line Managers
Training & Awareness	GDPR 8.2	b43	Medium	Create a procedure for following up non-completion of data protection and information security training across SPA, clearly allocating responsibility for training follow up as appropriate. This process should be consistent across the organisation and reported centrally.	Partially Accepted	We will be ensuring that all SPA staff are aware of our role in training and we will be reporting on training to the relevant management group.	Jan-18	Head of IM
Data Sharing	GDPR 6.2	c1	High	Create an information sharing policy that clearly sets out who has the authority to make decisions about systematic sharing or one-off disclosures, and when it is appropriate to do so. This should include general principles to consider when sharing SPA information and the roles and responsibilities assigned within the organisation for information sharing. Also include a template DSA and guidance for completing DSAs. As part of the review and monitoring of compliance with this policy, SPA should conduct dip samples to ensure sharing is proportionate to the purpose and decisions are being recorded by following the audit trail from request through to disclosure. See the ICO Data Sharing Code of Practice and Data Sharing Checklists for further guidance.	Accepted	Blank	Dec-18	Head of IM

Data Sharing	GDPR 2.3	c2	Urgent	SPA should identify all agencies with which they regularly share information. Formal data sharing agreements should be established as a matter of urgency. These agreements should: - set out common rules to be followed by all partners in the sharing be signed off by a senior staff member, for example the CEO; - specify how long shared data is to be retained for before it is to be returned to the data controller or securely destroyed; - specify security arrangements relating to the transfer of shared data and access to shared data; and - be subject to regular review to ensure partner organisations are removed from or added to agreements when required, and to regularly examine the working of the agreement.	Rejected			
Data Sharing	GDPR 2.1	c4	High	All sharing decisions should be recorded (i.e. reasons, purpose, decision making process and rationale) providing a complete audit trail should the decision to share or not to share be challenged.	Rejected		No date	No owner
Data Sharing	GDPR 6.8	c5	High	SPA should ensure that staff are adequately trained in recognising requests for information and responding appropriately, for example, by directing all requests to the Information Management Team. SPA should ensure generic and role-based training needs are identified and met on appointment and, where appropriate, periodically thereafter. Please refer to recommendation at b10 regarding training needs analysis.	Accepted		Jan-18	Head of IM
Data Sharing	GDPR 4.1	c6	Urgent	SPA should make fair processing information about sharing and the purpose shared readily available to data subjects, unless an exemption applies, for example via the SPA website. Where necessary, fair processing information should be actively communicated to individuals and their consent to share information with third parties sought. Further information about privacy notices under the GDPR is available on the ICO website.	Accepted		Nov-17	Head of IM / Head of Complaints
Data Sharing	GDPR 2.1 & 4.1	c7	High	Retrospective PIAs should be completed in relation to current data sharing. Include requirement in Information Sharing policy recommended at c1. To ensure that sharing is fair and lawful, instances of sharing should be considered on a case by case basis and a clear justification of how such exchanges of data fulfil the requirements of the DPA recorded. In addition, where necessary, condition(s) for processing should be recorded.	Partially Accepted	Recommendation is rejected if it is related to c2. If it relates to the ad-hoc disclosures being made by FS then it is accepted. We have shut down all sharing (if there was indeed any) that isn't required by law, instructed by the data controller or done under defence access policy. We don't think there was any ad hoc disclosures. We were making disclosures, but only those that PSoS told us to make.	No date	No owner
Data Sharing	GDPR 2.1 & 4.1	c8	High	SPA should assess and document the legal basis for regularly sharing information with third parties. This should form part of the PIA (see recommendation c7) and included in the DSA.		Not accepted for C2, but if its ad-hoc then accepted	No date	No owner
Data Sharing		c9	Urgent	See recommendation at c2. The requirement to have DSAs in place should be documented in policy. Relevant staff should be made aware of this requirement. Retrospective DSAs should be completed for current sharing agreements.	Rejected			
Data Sharing	GDPR 2.2	c10	Urgent	See c2. SPA should introduce a DSA with PSoS as a matter of urgency. Please refer to recommendation at c9.	Rejected		No date	No owner
Data Sharing	GDPR 2.2	c11	Urgent	SPA should ensure that all regular information sharing is documented and controlled through a DSA. SPA should take a proactive approach by sending a Data Sharing Survey to all business areas including Forensic Services to detail any information sharing they are involved in to identify gaps and enable the provision of advice and guidance with creating a formal DSA. The completion of the data sharing survey task by all business areas should be mandated and tracked through the appropriate forum with regular reports on progress provided to the SIRO by the HoIM.	Accepted	Blank	Dec-17	Head of IM

Data Sharing	GDPR 2.2	c12	High	See C2. In addition to the agreements themselves, SPA should have statements of compliance signed by senior management of each party involved in the sharing. SPA should conduct regular compliance checks with sharing partners to ensure the terms of the agreement and framework is being adhered to and any issues raised should be reported to the appropriate forum/SIRO.	Accepted	Accepted where C11 identifies any relevant sharing	no date	Head of IM
Data Sharing	GDPR 2.2	c13	High	Once DSAs are completed and authorised by the HoIM/SIRO introduce a review process to ensure partner organisations are removed from or added to agreements when required, and to regularly examine the working of the agreement. See C2.	Rejected	Blank		
Data Sharing	GDPR 2.2 & 4.1	c14	High	See C2. Once DSAs are in place, these should be centrally logged to ensure oversight of agreements and that they are regularly reviewed and kept up to date.	Accepted	When/if the first new DSA is completed then the recommendation will have been discharged. We can't give a date as we don't have any agreements to log as yet.		Head of IM
Data Sharing	GDPR 2.2	c16	High	SPA should implement formal processes to ensure that shared data is kept accurate and up to date. Ensure staff who are actively sharing data with other agencies are conducting data quality checks on the information prior to sharing and if appropriate inform recipients when any amendments or updates are made.	Rejected	SPA does not create source personal data, this is provided by 3rd parties	No date	No owner
Data Sharing	GDPR 2.2	c17	High	SPA should ensure the storage and destruction of the data is aligned with their own retention and disposal policy/schedule and details the specific arrangements in each DSA.	Rejected			
Data Sharing	GDPR 2.2	c18	High	SPA should ensure all agreements specify the protective marking to be applied to the data before being shared. This will ensure a level of sensitivity is understood particularly if different organisations have different standards.	Accepted	Blank	As and when written	Head of IM
Data Sharing	GDPR 2.2	c19	Urgent	Please refer to recommendation at c2.	Rejected			
Data Sharing	GDPR 5.3	c20	High	Please refer to recommendation at a90. DSAs should include the requirement to report all actual and potential security incidents and 'near misses' to the Information Management team so that they can be investigated and resolved appropriately.	Rejected		No date	No owner
Data Sharing	GDPR 2.1 & 2.2	c21	High	SPA should devise a policy for all staff in relation to disclosures of personal data include requirements in the policy recommended at 1. This should include the steps that should be taken to verify the validity of the request, the requirement for disclosures to be recorded on Evidence Management System EMS) and who is able to authorise one off disclosures to third parties.	Accepted	Blank	Jan-18	Director of Forensic Services
Data Sharing		c22	High	SPA should ensure that all one off verbal or written disclosures to third parties are logged on EMS or other relevant system, including the legal basis for disclosure. Managers should conduct spot checks or compliance reviews. See C1.	Accepted	Blank	Jan-18	Director of Forensic Services / Head of IM
Data Sharing	GDPR 3.2	c27	High	As Data Controller, SPA should ensure they have central oversight/governance of security incident management and follow up with all business areas. This will ensure all incidents involving personal data are satisfactorily resolved and that lessons learned are communicated to staff. In addition any risks identified during investigations can be monitored and mitigated against by the HoIM/SIRO consistently on an ongoing basis.	Accepted	ICO Comment SPA did not provide the ICO with any indication of acceptance of recommendation or data for implementation.	No date	PSoS
Data Sharing		c29	Medium	SPA should monitor compliance with these policies.	Rejected			

NO GDPR EQUIVALENT

ICO REPORT MORE GRANULAR THAN GDPR