SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee**
Date	**24 July 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**ICO Audit Update**
Item Number	**6.3**
Presented By	**Lindsey McNeill**
Recommendation to Members	**For Information**
Appendix Attached	**A. ICO Recommendation Tracker**

PURPOSE

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 Approval** in relation to update on progress against ICO recommendations.

1. BACKGROUND

1.1 The Audit Committee previously viewed the ICO Audit Report at its Committee Meeting convened in June 2018. This report is an update on progress against the specific actions detailed in that report, and indicates future work still required.

1.2 ICO have been sent a copy of the updated action plan on 16 July 2018, and SPA await their response in relation to follow up audit work due in October 2018.

1.3 Onwership of all outstanding actions has now been transferred to the new Information Governance Forum, chaired by the SPA Senior Information Risk Owner (SIRO).

1.4 Going forwards, the Information Governance Forum will report progress on relevant action plans and ongoing compliance to the SPA Audit Committee on a six-monthly basis.

2. GENERAL PROGRESS UPDATE

2.1 Since the date of the last Audit Committee meeting, a cross check of all available information and work carried out under the auspices of the GDPR-readiness project has been completed. This has been matched to the ICO recommendations and can be viewed in the attached appendix.

2.2 In reviewing the content of the ICO Report, the following updates were made:

- Of the 117 recommendations, SPA can AGREE with 114 Recommendations and PARTIALLY AGREE with 3 recommendations. There are none which SPA would reject.

- 44 actions are completed in full, the rest have had significant work undertaken on them, and this breaks down into:
    - 13 of the ICO-rated 'Urgent' priority actions have been completed from 28.
    - 23 of the ICO-rated 'High' priority actions have been completed from 72.
    - 4 of the ICO-rated 'Medium' priority actions have been completed from 10.
    - 4 of the ICO-rated 'Low' priority actions have been completed from 7.

3. FINANCIAL IMPLICATIONS

3.1 There are no additional financial implications in this report beyond those previously reported.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications associated with this paper.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications associated with this paper.

5.2 While not directly associated with the content of this paper, the non-compliance of SPA with the ICO audit recommendations and the GDPR legislation may result in penalties for SPA.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no direct reputational implications associated with this paper. However, failure to comply with the legislation and any resulting publicity may have reputational implications in the current climate.

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 are no equality implications associated with this paper.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications associated with this paper.

RECOMMENDATIONS

Members are requested to:

1. Note the progress to date in relation to actions to address the ICO report; and,

2. Note that the Information Governance Forum will now report progress of activities to the Audit Committee on a 6-monthly basis.

Appendix A – ICO RECOMMENDATION TRACKER – AS AT 25 JUNE 2018

Scope Area	Finding No	Priority	Recommendation	Accepted / Partially Accepted / Rejected	Agreed Action	Implementation Date	Owner	Update at end of June 2018 (3 months post publication)	Evidence to support position
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, however the agreed temporary acting up responsibility was to cover fully for the Director of Governance and Assurance. Therefore, it was implicit by the individual taking on the responsibility that the role of SIRO would be covered.	Dec-16	Head of Legal in agreement with Director of Governance & Assurance	An interim Director was appointed during this time, and her role descriptor included this responsibilty. The permanent Director has now returned to work and will resume these responsibilties. This action has now been superseded. **ACTION COMPLETED**	**CHANGE REJECTION TO PARTIALLY ACCEPTED** **Evidence:** **1. Interim Director Job Description** **2. Actions of Director of Governance & Assurance since return**
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	**Revised SOP finalised.** **ACTION COMPLETED**	**Evidence:** **1. Revised SOP**
Security of Personal Data	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	Our information Asset Register is now complete and the appropriate data sharing agreements have been drafted. **Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016.	**Evidence:** **1. Draft Section 83 / Shared Services Agreement** **2. Data Sharing Agreement as required by GDPR legislation - SPA is a DATA CONTROLLER**

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	Review the current actions associated with the SPA Risk Management Policy in light of this recommendation - this includes creation of a SPA Strategic Risk Register which would replicate that format used in Forensics and Police Scotland.	Jun-18	Risk & Policy Manager	There is a high level risk management policy In place, previously approved by the SPA Audit Committee in 2015. The current direction of travel in relation to Tolerance and Appetite is a request from the Board Members over a period of time. Consideration relevant to issues contained in ICO recommendations will be included in this context. **Action Still Required:** Set risk appetite and tolerance levels within SPA and ensure mitigation is aligned to appetite and tolerance.	**CHANGE REJECTION TO PARTIALLY ACCEPTED** **Evidence:** **1. Audit & Risk Committee Minutes detailing previous audit discussions (DATE TBC)** **2. Audit & Risk Committee Terms of Reference / Workplan** ***3. Statement of tolerance / appetite levels for risk across Scottish Policing (to be started)***
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.	Dec-17	Risk & Policy Manager	GDPR Programme Risk Register was Complete December 2017.**Action Still Required:** Now require to transfer residual risks over to business as ususal SPA Corporate Risk Register., as well as considering additional risks relevant to Information Management	**Evidence:1. Meeting to discuss emerging risks in relation to IM is scheduled for 16 July 2018.2. Updated Risk Register**
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	Forensics Services to liaise with the SPA Risk & Policy Manager to ensure accuracy and escalation of all relevant risks, as per recommendation a11.	Jan-18	Director of Forensic Services	An overarching risk regarding information management for Forensics Services has now been included in the Corporate Risk Register. **ACTION COMPLETED**	**CHANGE PARTIAL TO ACCEPTED** **Evidence:** **1. Updated Risk Register**

Security of Personal Data	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	Create a Privacy Impact Assessment Policy	Nov-18	Head of IM	The PIA Notice was prepared for SMG approval in June 2015. These cover employees and members of the public and are on our website and intranet. **ACTION COMPLETED**	**Evidence:** **1.PIA Notices**
Security of Personal Data	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	Interim Director to attend Audit & Risk Committee Meetings to report on information security issues to the committee.	Complete by 1st Quarter 2018	Director of Governance and Assurance	Catherine Topley now attending and providing the audit committee with frequent updates, which have been publicised. ACTION COMPLETED	**Evidence:** **1.Audit & Risk Committee Minutes** **2. Security Incident Reports reported to Committee**
Security of Personal Data	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	Information Governance Forum to be established with Terms of Remit and workplan.	Nov-17	Director of Governance and Assurance	Draft TOR have been prepared and IGF will be established from July 2018 onwards - responsibility for carrying forward Business As Usual work from initial GDPR Project. **Action Still Required:** Schedule of meetings to be established and commenced.	**Evidence:** **1.IFG Terms of Reference** ***2. IFG Schedule of Meetings***
Security of Personal Data	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	CEO nominated Head of Information Mgt and Business Manager from Forensics to attend.	Will be in place for next scheduled meeting in 2018	CEO	Complete December 2017, LD to attend any relevant ICT meetings going forward. Further more Jennifer Muir also attends meetings with PSoS ICT to ensure Forensics needs are being considered at the appropriate time. **ACTION COMPLETED**	**Evidence:1. PSOS Working Group Minutes**

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	Review all policies to include review details.	Jan-18	Head of IM	Complete initial update to policy review dates undertaken in Jan 2018 All policies being reviewed for GDPR as per review cycle. **Action Still Required:** Final GDPR policies to be finalised. Once complete, will be sent to SMG for approval. Aim for end of July 2018.	**Evidence:** **1. List of policies with review dates in overall spreadsheet for tracking**
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 / SPA	There has been an increase in documents coming for review. The working relationship between PSoS has increased significantly and SPA continue to engage with this working relationship. There is cognisance that when arrangements may differ slightly from Police Scotland, an advice note will be issued to staff. **Action Still Required:** Ongoing review of policies and SOP's as they come into existence through Police Scotland - this will become Business as Usual	**Evidence:** **1. List of policies which require amendment to fit SPA requirements i.e. car hire usage**
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	**Action Still Required:** FS specific SOP's still to be shared with SPA Corporate for review	***Evidence:*** ***1. List of FS SOP's with overview by SPA IM. (TBC)***
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.	May-18	Director of Governance & Assurance	All information pertaining to SPA staff responsibilities to manage data safely are communicated through the SPA and PSOS intranet, through staff huddles and through email reminders from the Interim Chief Officer and the Director of Governance. **ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTED** **Evidence:** **1. PSOS Intranet Site** **2. SPA Intranet Site** **3. Moodle Training mandatory training** **4. Email reminders**

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	May-18	Head of IM	Qpulse is a Forensics system which records when people access certain policies / procedures / training. It does not hold the policies or SOP's themselves, but links into what is held on the SPA PSOS intranet site. **ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTEDEvidence:1. PSOS Intranet Site2. SPA Intranet Site3. Moodle Training mandatory training4. Email reminders5. Link to Qpulse system which records people accessing the information.**
Security of Personal Data	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	Induction checklists currently being developed (June 2018). **Action Still Required:** Ongoing review of policies and SOP's as they come into existence through Police Scotland - this will become Business as Usual Forensics Staff agreement and understanding of policies and procedures will be captured through Qpulse. Online test to be developed to ensure completion of training. SPA Corporate Staff and board members will be asked to sign a register to show they have understood all relevant policies and SOPS's following awareness training.	**Evidence:** **1. Induction checklist** **2. Qpulse records to show information captured for compliance** ***3. Policy register SPA Corporate and board members to sign to show understanding - still to be developed)***
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	Updated policies, SOPs and other associated agreements that were being reviewed as part of the GDPR work are being presented to the SPA SMT, starting in May 2018. **Action Still Required:** Remaining policies need reviewed by SMG before end of July 2018.	**Evidence:** **1. List of policies passed to SMG for approval with associated email sign off.**

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.	Dec-17	Director of Governance and Assurance	The requirement for passwords to be changed frequently is enforced through PSOS Group Policy regarding passwords. This applies to the STAGE 2 password as detailed in next column.The Bitlocker password is fixed but is designed to lock out any person attempting to put in the wrong access code 10 times. When the bitlocker encryption is enacted, it renders the laptop useless until such a time that a secure access code is entered by an IT administrator.The Network password prompts users to change their password every 30 days, and has to be a complaex password using alphanumeric and special characters.The RAS token password does not update. Should the token be misplaced or stolen, the IT department have the ability to 'sting it' to render it useless. It does not hold data in itself - it is a security key to enable network access only.**ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTEDEvidence:1. User evidence:STAGE 1 - Bitlocker password which controls the ability to log onto the laptop past the initial start up screen. STAGE 2 - Network password which controls the ability to log into the SPA / PSOS user account. STAGE 3 - RAS token password which controls the ability to log onto network and ability to access systems / documents.**
Security of Personal Data	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	Head of IM	Asset Register created, and all of SPA mobile devices, tablets, blackberries, mobile phones, MyFi wireless and RAS tokens are captured on this spreadsheet. This will be reviewed on a quaraterly basis to maintain accuracy. **ACTION COMPLETED**	**Evidence:** **1. SPA Mobile Asset Register**

Security of Personal Data	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	**Action Still Required:** SPA will create a user training note regarding use of mobile devices and responsibilities linked to agreed policies, and will require a register to be maintained to show compliance by users. Will be contained against the SPA Mobile Asset Register.	**Evidence:** **1. SPA Mobile Asset Register** ***2. Briefing note / face-2-face training to outline how to use mobile devices - still to be developed)*** ***3. Policy register SPA Corporate and board members to sign to show understanding - still to be developed)***
Security of Personal Data	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	**Action Still Required:** Spot checks will be carried out to show compliance by users. Will be contained against the SPA Mobile Asset Register to identify users.	**Evidence:** ***1. Spot check register SPA Corporate and board members to sign to show understanding (- still to be developed)***
Security of Personal Data	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	Creation of an Information Asset Register across all of SPA Corporate and Forensics.	Work will commence November 2017	Head of IM	Information Asset Register created across all of SPA Corporate and Forensics.**ACTION COMPLETE AS BASELINE** - Ongoing live document	**Evidence:1. SPA Corporate / Forensics Information Asset Register**

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	Owners to be assigned to all physical and electronic information assests identified in the Information asset register.	Dec-17	Head of IM/HR	Information asset owners are identified in Syops. As the role of IAO may be fluid it may not always be possible to record in job descriptions. **Action Still Required:** Through planned structure reviews within SPA Corporate (and possibly Forensics in the future) it *may* be possible to add in the IAO's as part of planned consultation with staff. To do so at present may detract from wider review of terms and conditions happening across the whole of SPA / Police Scotland. A more pragmatic approach is that IAO's are kept as a seperate register.	**Would suggest this be changed to a PARTIAL ACCEPTANCE? The issue is about inclusion of these roles within job descriptions.** **Evidence:** ***1. Information Asset Owner register for SPA Corporate and Forensics (still to be developed)***
Security of Personal Data	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	Review and update current Remote Working Policy and disseminate to staff.	Dec-17	Head of IM	New policy created by external lawyers, and approved by SMG in June 2018. **ACTION COMPLETED**	**Evidence:** **1. Updated Remote Working Policy** ***2. Email disseminating to staff?***
Security of Personal Data	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	**Action Still Required:** SPA will create a user training note regarding use of mobile devices and responsibilities linked to agreed policies, and will require a register to be maintained to show compliance by users. Will be contained against the SPA Mobile Asset Register.	**Evidence:** **1. SPA Mobile Asset Register** ***2. Briefing note / face-2-face training to outline how to use mobile devices - still to be developed)*** ***3. Policy register SPA Corporate and board members to sign to show understanding - still to be developed)***
Security of Personal Data	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	A log is maintaned in both FS and SPA corporate **ACTION COMPLETED**	**Evidence:** **1. Iron Key Register**

Security of Personal Data	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	**Action Still Required:** 28/5 Scene Examination have procured Secure Data Solution. Testing and deployment phase ongoing - target go live July 2018.	***Evidence:*** ***1. New system and new SD cards***
Security of Personal Data	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	New policy created by external lawyers, and approved by SMG in June 2018.**Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff.	**Evidence:1. Updated Access Control Policy*2. Underpinning procedures to be created.3. Email disseminating to staff?***
Security of Personal Data	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	**Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff.	**Evidence:** **1. Updated Access Control Policy** ***2. Underpinning procedures to be created.*** ***3. Email disseminating to staff?***
Security of Personal Data	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	This is being addressed through Police Scotland's ADEL rollout. SPA are next to be considered in the rollout plan but firm timescales to be confirmed. **Action Still Required:** Seek confirmation from PSOS IT in relation to likely timescales. Update likely at end of July 2018.	
Security of Personal Data	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	New policy created by external lawyers, and approved by SMG in June 2018. **Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff.	**Evidence:** **1. Updated Access Control Policy** ***2. Underpinning procedures to be created.*** ***3. Email disseminating to staff?***

Security of Personal Data	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	Link to a51 and a55. (There is no a52) New policy created by external lawyers, and approved by SMG in June 2018. **Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff, and the new SPA HR post wil be responsible for ensuring consistent application and that process is followed consistently.	***Evidence:*** ***1. Underpinning procedures to be created.*** ***2. Email disseminating to staff?*** ***3. New SPA HR post has responsibility for ensuring appropriate communications to action these processes.***
Security of Personal Data	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	**Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff.	**Evidence:** **1. Updated Access Control Policy** ***2. Underpinning procedures to be created.*** ***3. Email disseminating to staff?***
Security of Personal Data	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	**Action Still Required:** 28/5 FS have scoped a manual dip sampling process for access to EMS. In addition quote sought from Abbotts re 'Random Case Generator' which will auto generate for audit purposes. Either solution will be incorporated into FS Mgt System . Target date for closure July 2018. FS Lead EMS Development Manager.	**Evidence:*1. Log of Dip Sampling Exercise and any follow up action required***
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.	Q1 2018/19	Head of IM	Evidence was sent to the ICO, however was not considered. SPA and Forensics already undertake this activity and have historical evidence to demonstrate. **ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTED** **Evidence:** **1. Physical Security Audits** **2. Follow Up to Security Audit Recommendation**

Security of Personal Data	a61	Urgent	Please refer to recommendation at a60.	Rejected	See a60	Q1 2018/19	Head of IM	Evidence was sent to the ICO, however was not considered. SPA and Forensics already undertake this activity and have historical evidence to demonsrate. **ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTED** **Evidence:** **1. Physical Security Audits** **2. Follow Up to Security Audit Recommendation**
Security of Personal Data	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	Door access logs provided monthly by DS for PQ. **ACTION COMPLETED**	**Evidence:** **1. PQ Door Logs**
Security of Personal Data	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	Email sent out to all staff to remind them. Spot checks carried out and results recorded. **ACTION COMPLETED**	**Evidence:** **1. Emails to staff: Reminders sent out on a regular basis**
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	Secure cabinets have been identified. Staff reminded to lock information away, clear desk audits conducted. **ACTION COMPLETED**	**Evidence:** **1. Emails to staff: Reminders sent out on a regular basis** **2. Physical check of locked cabinets / locked offices**
Security of Personal Data	a72	Urgent	Please refer to recommendations at a69 and a71.	Accepted		Dec-17	Head of Legal	Secure cabinets have been identified. Staff reminded to lock information away, clear desk audits conducted. New additional storage also now arrived onsite. **ACTION COMPLETED**	**Evidence:** **1. Emails to staff: Reminders sent out on a regular basis** **2. Physical check of locked cabinets / locked offices**
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	**Action Still Required:** Handbook will be completely revised for GDPR to incorporate GDPR /LED requirements 2nd Q 2018	***Evidence:1. Updated Information Security SOP / Handbook (Still to be completed)***

Security of Personal Data	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.	Dec-17	Head of IM / ICT	Destruction remains a matter for PSoS, but SPA will ensure receipts are issued for the return of equipment to PSOS, and that the Information Asset Register is updated accordingly. **ACTION COMPLETED**	**Evidence:** **1. Information Asset Register** (Showing any returned equipment)
Security of Personal Data	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		Dec-17	Head of IM	SPA operate on this basis already, certificates are retained. **ACTION COMPLETED**	**Evidence:** **1. Secure Disposal Certificates**
Security of Personal Data	a80	Urgent	Please refer to recommendation at a69.	Partially Accepted		Dec-17	Director of Forensic Services	**Action Still Required:** 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 28/5/18 Action discharged to FS IS Group to identify Clear Desk Champions across FS sties; scope solutions where required and establish checking/reporting at each FS site. Target date for completion July 2018	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** **Evidence:** **1. Emails to staff: Reminders sent out on a regular basis**
Security of Personal Data	a81	Urgent	Please refer to recommendation at a71.	Accepted		Dec-17	Director of Forensic Services	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. **ACTION COMPLETED**	**Evidence:** **1. Emails to staff: Reminders sent out on a regular basis** **2. Physical check of locked cabinets / locked offices**

Security of Personal Data	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	This reflects the service back arrangements from PSOS IT. **Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016.	**Evidence:** **1. Draft Section 83 / Shared Services Agreement**
Security of Personal Data	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.	Jul-18	PSoS	This reflects the service back arrangements from PSOS Procurement, generating contracts on behalf of SPA, but also in SPA's name.**Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016.	**Evidence:1. Draft Section 83 / Shared Services Agreement**
Security of Personal Data	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.	Jul-18	PSoS / Director of Governance	**Action Still Required:** This will be a resource issue for SPA as its currently a service back from PSoS. SPA snr mgt will have to review this recommendation and decide on its requirement One suggestion may be to ensure that a legal clause is inserted into all supplier contracts which meets SPA information security requirements are discharged.	***Evidence:*** ***1. Draft legal wording inserted into contract discharging SPA Info Security Requirements?***

Security of Personal Data	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.	Jul-18	PSoS	This reflects the service back arrangements from PSOS Procurement, generating contracts on behalf of SPA, but also in SPA's name. **Action Still Required:** SPA to ascertain if this criteria is requested by Police Scotland in their tendering process.	***Evidence:*** ***1. Confirmation from PSOS Procurement in relation to data handling training criteria placed upon suppliers?***
Security of Personal Data	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.	Jul-18	PSoS	This reflects the service back arrangements from PSOS Procurement, generating contracts on behalf of SPA, but also in SPA's name. **Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016. Information to be passed to suppliers with regarding notifing SPA / PSOS of any information security incidents	***Evidence:*** ***1. Confirmation from PSOS Procurement in relation to what processes are in place for suppliers to report information security incidents.*** ***2. Confirmation that PSOS flag such incidents to SPA Info Mgt, and also to the Audit and Risk Committee through regular reporting.***
Security of Personal Data	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.	Jul-18	PSoS	This reflects the service back arrangements from PSOS Procurement, generating contracts on behalf of SPA, but also in SPA's name.**Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016.	**Evidence:1. Draft Section 83 / Shared Services Agreement**
Security of Personal Data	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.	Jul-18	PSoS	This is a service back from PSoS currently, in that PSoS reserves this right on our behalf. If SPA is to undertake this role it will have to be resourced. **Action Still Required:** SPA to check with PSOS if and when this occurs.	***Evidence:*** ***1. Confirmation from PSOS Procurement / IT / Info Mgt that they do conduct regular audits to ensure compliance with security requirements set out in the contracts.***

Security of Personal Data	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	The SPA Information Security Policy and the Data Incident Management Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Information Security Policy** **2. Data Incident Management Policy**
Security of Personal Data	a94	High	Please refer to recommendation at a97.	Accepted	Blank	Dec-17	Head of IM	The SPA Information Security Policy and the Data Incident Management Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Information Security Policy** **2. Data Incident Management Policy**
Security of Personal Data	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	The SPA Information Security Policy and the Data Incident Management Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Information Security Policy** **2. Data Incident Management Policy**
Security of Personal Data	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	The SPA Information Security Policy and the Data Incident Management Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Information Security Policy** **2. Data Incident Management Policy**
Security of Personal Data	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	The SPA Information Security Policy and the Data Incident Management Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Information Security Policy** **2. Data Incident Management Policy**
Security of Personal Data	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	**Action Still Required:** A lessons learned log will be created and communicated to staff quarterly.	***CHANGE PARTIALLY ACCEPTED TO ACCEPTEDEvidence:1. Lesson learned from Security Incidents Report to be generated quarterly.***

Security of Personal Data	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	Head of IM	**Action Still Required:** This report used to go to Audit & Risk Committee, and has been superseded by a joint report presented by Police Scotland. Reporting process will be reviewed going forwards.	***Evidence:*** ***1. Quarterly Reports on SPA Security Incidents from Director of Governance and Assurance***
Security of Personal Data	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	Head of IM	Initial work on GDPR preparation meant that external lawyers and a temporary internal resource were brought into SPA to make sure that new policies and procedures were created to meet the GDPR requirements. This has generated a whole new suite of policies which the Information Management Team will conduct security audits against in the coming months to test their efficacy **Action Still Required:** Schedule of info security audits to be scheduled by IM Team.	***Evidence:*** ***1. SPA IM programme of audits to check efficacy of IM security policies (work yet to be identified)***
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	Jul-18	PSoS	**Action Still Required:** Obtain audit of health check on SPA systems carried out by 3rd party supplier, on behlaf of PSOS. Requirement to understand where this now sits in the overall picture of PSOS IT now seeking GDPR compliance with all its systems.	***Evidence:*** ***1. Review previous PSOS audit and check if still relevant moving forwards.***
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	**Action Still Required:** Schedule of info security audits / spot checks to be scheduled by IM Team and recorded for audit purposes.	***Evidence:*** ***1. SPA IM programme of audits to check efficacy of IM security policies (work yet to be identified)***
Security of Personal Data	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	Jul-18	PSoS	This reflects the service back arrangements from PSOS IT. **Action Still Required:** Section 83 (Service Level Agreements) have been passed to Police Scotland again on 25/06/18 to Deputy Chief Operating Officer. Originally sent for consideration in November 2016.	**Evidence:** **1. Draft Section 83 / Shared Services Agreement**

Training & Awareness	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	Given the recent implementation of GDPR there has been significant oversight by the Audit and Risk Committee in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members.**ACTION COMPLETED**	**Evidence:1. Moodle training package2. Board training package3. Email notification and briefings to staff**
Training & Awareness	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.	Jul-18	Director of Governance and Assurance	Information Governance Forum established with Terms of Reference with first meeting scheduled for July. The Forum will take the outstanding actions as the basis for its workplan from both the ICO audit and the GDPR action plan items. **ACTION COMPLETED**	**Evidence:** **1.IFG Terms of Reference** ***2. IFG Schedule of Meetings***
Training & Awareness	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	28/5/18 DP and IS training now incorporated into FS Training Needs Analysis (approved at OM Forum May 2018). DP training roadshows provided by SPA IM to FS staff in May 2018 - further dates to be confrimed. List of staff that have completed training to date to be provided by SPA IM to FS. FS to action update to Scope as well at T&C Records. **ACTION COMPLETE**	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** **Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**

Training & Awareness	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.	Jul-18	Head of IM	SPA are currently undergoing an Executive Review of its structure. As part of this process, job descriptions are being updaed to reflect this. Currently in consultation. Assuming acceptance, this action will be discharged at the end of the consultation period. **Further action required:** Once there is a final agreed structure, this action can be closed	***Evidence:*** ***1. Updated job descriptions***
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	Jul-18	Head of IM	Given the recent implementation of GDPR there has been significant work in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members.**ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTEDEvidence:1. Moodle training package2. Board training package3. Email notification and briefings to staff**
Training & Awareness	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	Given the recent implementation of GDPR there has been significant work in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members. **ACTION COMPLETED**	**CHANGE REJECTION TO ACCEPTED** **Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**

Training & Awareness	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.	Oct-18	PSoS	Given the recent implementation of GDPR there has been significant work in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members. **Further action required:** Once the new HR post is recruited, a more regular programme of TNA's require to be conducted across SPA.	**Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff** ***4. TNA and training strategy established for SPA***
Training & Awareness	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.	Oct-18	PSoS	**Further action required:** Once the new HR post is recruited, a more regular programme of TNA's and preparation of a training strategy requires to be prepared across SPA.	***Evidence:*** ***1. TNA and training strategy established for SPA***
Training & Awareness	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	The SPA Data Protection Policy was prepared for SMG, and approved in June 2015. **ACTION COMPLETED**	**Evidence:** **1. SPA Data Protection Policy**
Training & Awareness	b14	High	Induction checklists should be submitted centrally so Information Management have oversight of its effectiveness.	Rejected		Oct-18	Head of IM	**Further action required:** Once the new HR post is recruited, a more regular programme of TNA's and preparation of a training strategy requires to be prepared across SPA.	**CHANGE REJECTION TO ACCEPTED** ***Evidence:*** ***1. Induction checklist for new starts*** ***2. TNA and training strategy established for SPA***

Training & Awareness	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	Oct-18	Head of IM	Link to a27. Handbook essentially IS all the Information Management Policies.**Action Still Required:** Ongoing review of policies and SOP's as they come into existence through Police Scotland - this will become Business as Usual. Forensics Staff agreement and understanding of policies and procedures will be captured through Qpulse. Online test to be developed to ensure completion of training. SPA Corporate Staff and board members will be asked to sign a register to show they have understood all relevant policies and SOPS's following awareness training.	**CHANGE PARTIALLY ACCEPTED TO ACCEPTEDEvidence:1. Induction checklist2. Qpulse records to show information captured for compliance*3. Policy register SPA Corporate and board members to sign to show understanding - still to be developed)***
Training & Awareness	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	SPA IM Team carried out roadshows with staff and have signed registers of those attended. This is work in progress but so far ~ 80% of forensics staff have been covered, and all Board Members have received face to face training. **Action Still Required:** Completion of roadshows for the remaining member of staff.	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** **Evidence:** **1. Induction checklist** **2. Qpulse records to show information captured for compliance** **3. Attendance register for training** ***4. Policy register SPA Corporate and board members to sign to show understanding - still to be developed)***

Training & Awareness	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.			Jul-18		Given the recent implementation of GDPR there has been significant work in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members. **ACTION COMPLETED**	**Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**
Training & Awareness	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	New package developed in order to be GDPR compliant and used currently. Improvements will include an online test and additional information. **ACTION COMPLETED**	**Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**
Training & Awareness	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	**Action Still Required:** Test to be designed and implemented	***Evidence:1. Online test available and used (TBC)***
Training & Awareness	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	Jul-18	Head of IM	Given the recent implementation of GDPR there has been significant work in this area. This has included strong leadership within both SPA Corporate and Forensics regarding staff briefing sessions, online moodle training and also dedicated training sessions with Board Members. **ACTION COMPLETED**	**Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**
Training & Awareness	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		Oct-18	Head of IM	New package developed in order to be GDPR compliant and used currently. Improvements will include an online test and additional information. **ACTION COMPLETED**	**Evidence:** **1. Moodle training package** **2. Board training package** **3. Email notification and briefings to staff**

Training & Awareness	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.	Jul-18	PSoS	**Action Still Required:** Supporting procedures are still being developed, but once in place these will be communicated to staff.	**Evidence:** **1. Updated IM Policies** ***2. Underpinning procedures to be created for starters, movers and leavers*** ***3. Email disseminating to staff?***
Training & Awareness	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	Jul-18	Head of IM	Moodle already is available across the whole organisation. **ACTION COMPLETED**	**Evidence:** **1. Moodle training package** **2. Intranet notices** **3. Email notification and briefings to staff**
Training & Awareness	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	Oct-18	b25 - Head of IM b26 - CEO	**Further action required:** Once the new HR post is recruited, a more regular programme of TNA's and preparation of a training strategy requires to be prepared across SPA.	***Evidence:*** ***1. TNA and training strategy established for SPA***
Training & Awareness	b27	Low	Develop a checklist to ensure a consistent approach when responding to requests.	Rejected		May-18	Head of IM	New policies prepared with flowcharts to aid understanding of how to process requests within SPA. **ACTION COMPLETED**	**CHANGE REJECTED TO ACCEPTED** **Evidence:** **1. New FOI and DPA policy and associated flowcharts**
Training & Awareness	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	New policies prepared with flowcharts to aid understanding of how to process requests within SPA. In addition, these proocedures are explained within the IM training. **ACTION COMPLETED**	**Evidence:** **1. New FOI and DPA policy and associated flowcharts**
Training & Awareness	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	**Further action required:** Feedback forms on IM training will be created and used for future training events.	***Evidence:1. Analysis of IM training forms***
Training & Awareness	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	Intranet page has been updated to include all new policies. There are plans for a more significant refresh of the whole SPA website in due course but date TBC. **ACTION COMPLETED**	**Evidence:** **1.Updated intranet and internet pages relevant to IM.**

Training & Awareness	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	28/5 The FS quality manager will look at the possibility of using Q Pulse across the estate - **Further action required:** *update requested by SPA IM*	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** ***Evidence:*** ***1. SPA Corporate Access to Qpulse or a rejection by the supplier.***
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		Jul-18	Head of IM	Moodle already is available across the whole organisation which captures completion of mandatory training onto individual HR Scope Records. **ACTION COMPLETED**	**CHANGE REJECTED TO ACCEPTED** **Evidence:** **1. Moodle training package** **2. Intranet notices** **3. Email notification and briefings to staff**
Training & Awareness	b38	High	SPA should ensure that training completion is accurately recorded on staff scope records and kept up to date.	Accepted	Blank	Jul-18	Line Managers	**Further action required:** Communication to go out to staff to check that mandatoary training HAS been confirmed onto Scope Record, and if not, to ask their managers to engage with the Scope team directly.	***Evidence:*** ***1. Email to staff re: checking personal HR record.***
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		Oct-18	Line Managers	**Further action required:** Stats should be provided to SPA IM so an audit can be maintained in relation to data and info security.	**CHANGE REJECTED TO ACCEPTED** ***Evidence:*** ***1. Quarterly updates from Forensics to SPA IM team for collation and oversight***
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	Oct-18	Director of Governance & Assurance	**Further action required:** Once the new HR post is recruited, KPI's can be established	**CHANGE REJECTED TO ACCEPTED** ***Evidence:*** ***1. Quarterly updates from Forensics to SPA IM team for collation and oversight***
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	Mar-19	Director of Governance & Assurance	**Further action required:** Once the new HR post is recruited, the individual can work with line managers to capture all necessary information within PDC's.	**CHANGE REJECTED TO ACCEPTED** ***Evidence:*** ***1. Quarterly updates from Forensics to SPA IM team for collation and oversight***

Training & Awareness	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	Jul-18	Head of IM / Line Managers	**Further action required:** Policies and procedures are in place, and dip sampling audits should be undertaken by the IM Team.	**Evidence:1. Moodle training package2. Intranet notices3. SPA Policies and Procedures**
Training & Awareness	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.	Jul-18	Head of IM	**Further action required:** Policies and procedures are in place, and dip sampling audits should be undertaken by the IM Team.	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** ***Evidence:*** ***1. Quarterly updates from Forensics to SPA IM team for collation and oversight***
Data Sharing	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	**Further action required:** Following updated legal advice on back of GDPR work, it has now been confirmed that SPA is a DATA CONTROLLER. In some instances this will be in the singular, and in some cases we may be JOINT DATA CONTROLLERS with Police Scotland. This action will be covered data controller / data processor agreements currently being drawn up by external lawyers.	**Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**
Data Sharing	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		Dec-18	Head of IM	Data Sharing Register - **COMPLETE** Further action required: This action will be covered by the data controller / data processor agreements currently being drawn up by external lawyers.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**

Data Sharing	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		Dec-18	Head of IM	Data Sharing Register - **COMPLETE** **Further action required:** This action will be covered by the data controller / data processor agreements currently being drawn up by external lawyers.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**
Data Sharing	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	Training, awareness, changes to policies and procedures and ongoing staff huddles within SPA PQ confirm that all staff recognise what a request for info looks like and how to respond. COMPLETE and ONGOING**Further action required:** Further work required in Forensics to ensure awareness is at same level.	**Evidence:1. FOISA Policy2. Staff briefings and training*3. TNA for SPA staff***
Data Sharing	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	The PIA Notice was prepared for SMG approval in June 2015. These cover employees and members of the public and are on our website and intranet. **ACTION COMPLETED**	**Evidence:** **1.PIA Notices**
Data Sharing	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.	Mar-19	Head of IM	Data Sharing Register - **COMPLETE** **Further action required:** This action will be covered initiallt by the data controller / data processor agreements currently being drawn up by external lawyers., and then an assessment will have to be completed in respect of historical / retrospective PIA's.	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**

Data Sharing	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 Data Sharing Agreement.		Not accepted for C2, but if its ad-hoc then accepted	Mar-19	Head of IM	Data Sharing Register - **COMPLETE** **Further action required:** This action will be covered initiallt by the data controller / data processor agreements currently being drawn up by external lawyers., and then an assessment will have to be completed in respect of historical / retrospective PIA's.	**CHANGE PARTIALLY ACCEPTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**
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		Mar-19	Head of IM	Data Sharing Register - **COMPLETE** **Further action required:** This action will be covered initiallt by the data controller / data processor agreements currently being drawn up by external lawyers., and then an assessment will have to be completed in respect of historical / retrospective PIA's.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**
Data Sharing	c10	Urgent	See c2. SPA should introduce a DSA with PSoS as a matter of urgency. Please refer to recommendation at c9.	Rejected		Oct-18	Head of IM	Data Sharing Register - **COMPLETEFurther action required:** This action will be covered initiallt by the data controller / data processor agreements currently being drawn up by external lawyers., and then an assessment will have to be completed in respect of historical / retrospective PIA's.	**CHANGE REJECTED TO ACCEPTEDEvidence:*1. Signed Data Sharing Agreements with relevant partners* 2. Data Sharing Register**
Data Sharing	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	Jul-18	Head of IM	Data Sharing Register - **COMPLETE** Information Asset Audit **- COMPLETE** Information was assessed through the GDPR Project Board and is now being passed over to the Information Governance Fourm for onward scrutiny. **ACTION COMPLETED**	**Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**

Data Sharing	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	Oct-18	Head of IM	**Further action required:** This action will be considered by the external lawyers for inclusion in any Data Sharing Agreements.	**Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** ***2. Statements of Compliance***
Data Sharing	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	Mar-19	Head of IM	**Further action required:** This action will be covered initially by the data controller / data processor agreements currently being drawn up by external lawyers, and then a new process instigated for regular reviews	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Updated Data Sharing Register***
Data Sharing	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.	Oct-18	Head of IM	**Further action required:** Once signed DSA's received, these will be logged and enterd into a register with annual review dates.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Updated Data Sharing Register***
Data Sharing	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	Mar-19	Head of IM	**Further action required:** New procedures to be prepared once the scope of shared data is understood and how this can be quality assured.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. New process for quality assuring data prior to passing onto agreed parties***
Data Sharing	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		Mar-19	Records Manager	**Further action required:** Assurance required to make sure that physical storage and destruction is carried out in compliance with the PSOS SOP and/or specific arrangements within each DSA/	**CHANGE REJECTED TO ACCEPTEDEvidence:*1. Compliance with PSOS SOP2. Compliance with individual DSA requirements***

Data Sharing	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	**Further action required:** We have the OFFICIAL marking scheme which is used on all our documents - other organisations may not have similar schemes - we need to assess on case by case basis and share our policy. Data Sharing Agreements will be updated with GSC requirements.	**Evidence:** ***1. SPA-led Data Sharing Agreements with our protective marking scheme embedded.***
Data Sharing	c19	Urgent	Please refer to recommendation at c2.	Rejected		Oct-18	Head of IM	Data Sharing Register - **COMPLETE** Further action required: This action will be covered by the data controller / data processor agreements currently being drawn up by external lawyers.	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Sharing Register**
Data Sharing	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		Oct-18	Head of IM	**Further action required:** Data Incident Management Policy, this clarifies the procedure for reporting near misses. This will also be included in the DSA's	**CHANGE REJECTED TO ACCEPTED** **Evidence:** ***1. Signed Data Sharing Agreements with relevant partners*** **2. Data Incident Management Policy**
Data Sharing	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	**Further action required:**	**Evidence:** ***1. Forensic-specific policy on information disclosure?***
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	**Further action required:**	**Evidence:** ***1. Forensic-specific policy on information disclosure?***
Data Sharing	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.	Oct-18	Head of IM	**Further action required:** Clarification from PSOS IT to inform SPA IM when security breaches occur through misuse of email.	**Evidence:** ***1. Log of SPA Incidents Identified by PSOS IT*** **2. Data Incident Management Policy**

Data Sharing	c29	Medium	SPA should monitor compliance with these policies.	Rejected		Mar-19	Head of IM	**Further action required:** Dip sampling work to be conducted by SPA Information Management	**CHANGE REJECTED TO ACCEPTEDEvidence:***1. Dip sampling of compliance against all information management / data / gdpr relevant policies across SPA Corporate and Forensics*