SCOTTISH POLICE AUTHORITY

Agenda Item 2e

Meeting	**SPA Audit , Risk and Assurance Committee**
Date	**Wednesday 5 May 2021**
Location	**By Video Conference**
Title of Paper	**ICO report: SPA progress update**
Presented By	**John McNellis** **SPA Head of Finance, Audit & Risk**
Recommendation to Members	**For consultation**
Appendix Attached	**Appendix A – ICO progress update**

PURPOSE

This report provides the Committee with a full overview of the Information Commissioners audit of SPA corporate / forensics services and an update on the progress of implementing the findings from their audit.

The paper is presented in line with the corporate governance framework of the Scottish Police Authority (SPA) and committee terms of reference and is submitted for consultation.

1. BACKGROUND

1.1 In 2018 the SPA invited the ICO to carry out a consensual audit to assess compliance with the newly implemented data protection legislation with a focus on three broad areas: information security, data sharing and training.

1.2 The audit was finalised in December 2018 and ICO found a "***reasonable level of assurance*** *that processes and procedures are in place and are delivering data protection compliance*".

1.3 The audit identified "*some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation*".

1.4 The original report was submitted to ARAC and ongoing progress has been included in the SPA's audit and improvement reports to ARAC.

1.5 In January 2021, ARAC requested a specific report providing further detail on the progress of ICO recommendations.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 A report outlining the findings and progress to date is shown at **appendix A**.

2.2 The SPA has discharged 80% of recommendations (comprised 65% completed and 15% to be closed).

2.3 A revised implementation plan with completion dates for the remaining recommendations is outlined in the appendix. A number of the outstanding recommendations are reliant on the delivery of actions or work by Police Scotland which the SPA is continuing to progress.

3. FINANCIAL IMPLICATIONS

3.1 There are no financial implications associated with this report.

4. PERSONNEL IMPLICATIONS

4.1 There are personnel implications associated with this paper. The discharge of some actions is subject to additional resources to assist the current information management team.

5. LEGAL IMPLICATIONS

5.1 There are no specific legal implications in this paper. However, the ICO can undertake enforcement on organisation that fail to meet information rights obligations.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no specific reputational implications associated with this paper.

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 note the update on progress of ICO recommendations.

SCOTTISH POLICE AUTHORITY

Appendix A

Information commissioner (ICO) progress update

MAY 2021

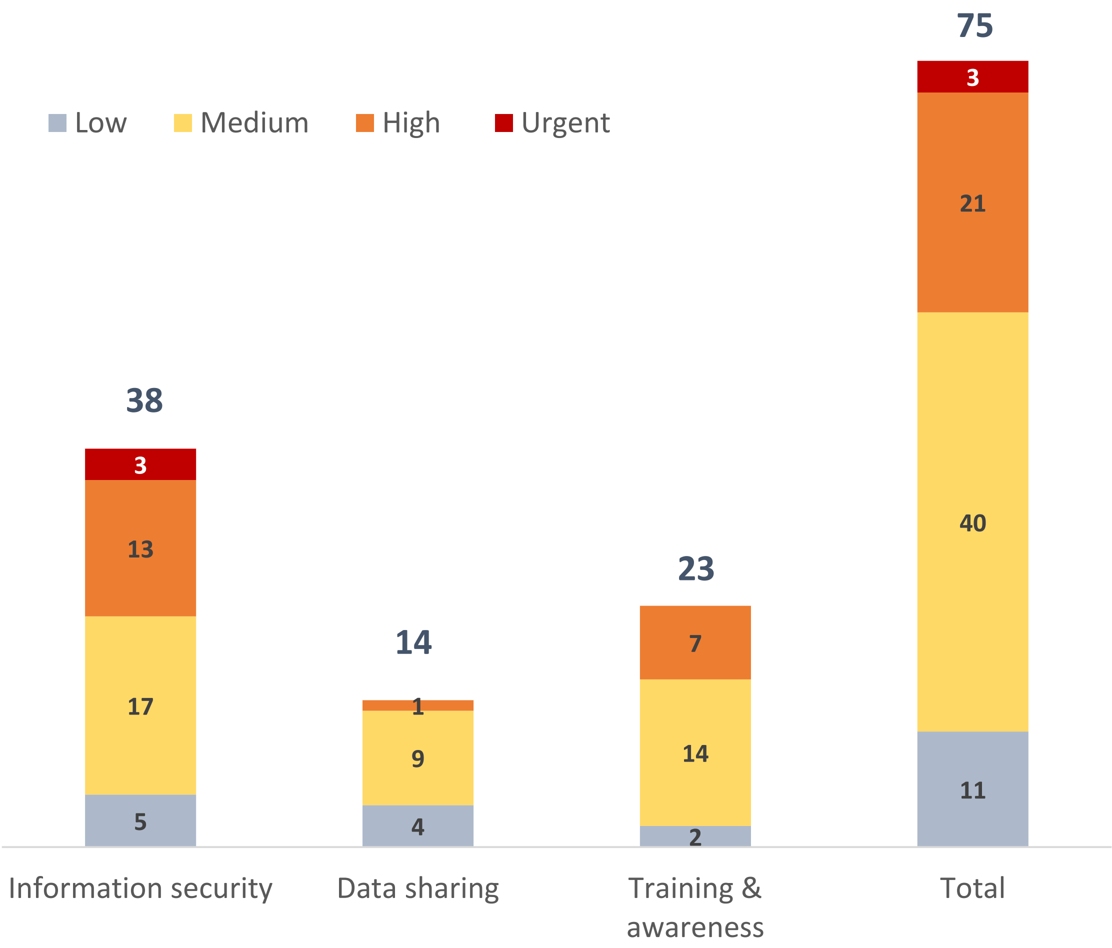
Background

The Information Commissioner (ICO) is responsible for enforcing and promoting compliance with the Data Protection legislation in the UK. The Data Protection Act allows the ICO to conduct consensual and compulsory audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

In 2018 the SPA invited the ICO to carry out a **consensual audit** to assess compliance with the newly implemented data protection legislation with a focus on three broad areas. The audit was finalised in December 2018 as the finding are summarised below.

These findings have been monitored by management and reported regularly to the Audit, Risk and Assurance Committee (ARAC) which requested a detailed report on progress. ICO carried out a formal follow up audit in December 2020 and has now concluded its involvement in this consensual audit.

Summary of original recommendations made



Scope area	Description	Rec's	ICO assurance	ICO overall opinion
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.	38	Reasonable assurance	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 data protection legislation.
Data sharing	The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.	14		
Training & awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.	23		
		75		

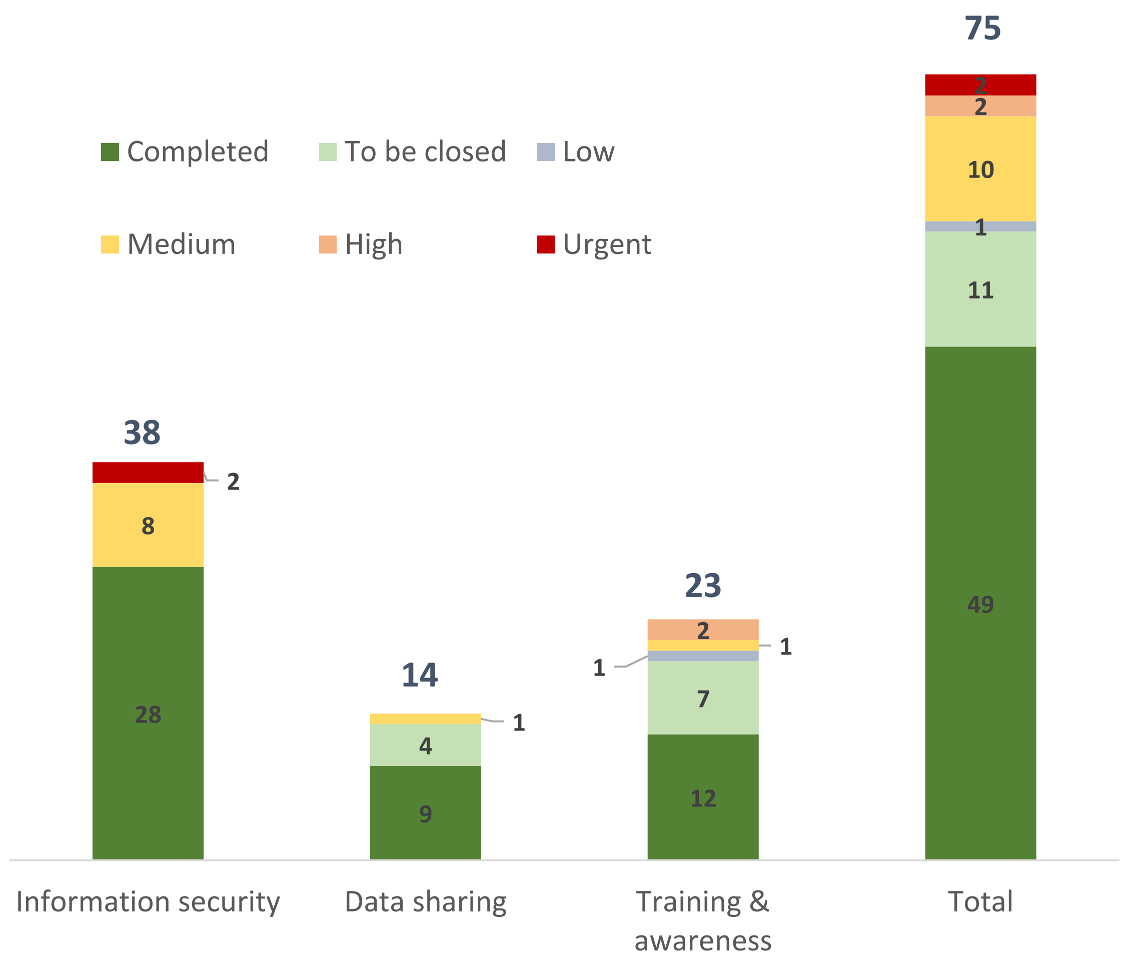
Recommendations progress

The SPA agreed to an action plan for all recommendations and has been working to progress each action. To date the SPA has discharged 80% of recommendations (comprised 65% completed and 15% to be closed). A number of the outstanding recommendation are also dependent upon the support of Police Scotland and in particular the Police Scotland ICT department.

There a four urgent or high risk recommendations that remain outstanding.

- The two urgent actions will be discharges when as83 agreement is reached with Police Scotland. There is a draft agreement in place that is currently being evaluated by Police Scotland.
- The two high risk actions relate to training and will be discharged following the completion of the SPA's training needs assessments and release of an updated elearning package.

Summary of recommendations (current progress)



Scope area	Total Rec's	Completed	To be closed	Outstanding
Information security	38	28	0	10
Data sharing	14	9	4	1
Training & awareness	23	12	7	4
	75	**49**	**11**	**15**
		65%	*15%*	*20%*

Scope area	Total Rec's	Completed	To be closed	Outstanding
Urgent	3	1	0	2
High	21	16	3	2
Medium	40	24	6	10
Low	11	8	2	1
	75	**49**	**11**	**15**

Recommendations to close

This provides further detail on recommendations to be closed.

Recommendations to close

The ICO recommendations were prepared over two years ago. The SPA in terms of the service and operating environment has changed over this period such that some recommendations are no longer applicable or have been realised in another way.

The follow table summarises recommendations the SPA is closing in addition to rational for this decision and how the risk is being mitigated if applicable.

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
C3	The forensics department have an existing Training Needs Analysis (TNA) process that includes IG training needs but it was reported that the TNA for SPA corporate staff is a work in progress. A new HR & Organisational Development Officer was appointed in October 2018 to develop the TNA.	a) SPA should ensure that training needs for all staff across the organisation are regularly assessed and identified. This will help them to identify any gaps in knowledge that can be addressed in their IG training programme. b) Staff responsibilities for the TNA process should be documented in relevant job descriptions.	High	*Recommendation relates to SPA Corporate only.* There are no corporate services staff with access to data that would require additional training and no-one outside IM is responsible for making decisions around disclosing/sharing data.
C9	Induction training is mandatory for all staff including temporary and individual contractors. This is not the case for staff providing security and cleaning services via a third party provider. Procurement of contracts for these services is done by PSoS in SPA's name as PSoS cannot legally enter into contracts. There is no requirement for the staff of these providers to undergo any induction training with respect to their responsibilities when handling personal data.	SPA should review contracts to ensure that they include the requirement for all staff employed by third parties to undergo data protection training appropriate to their role. Alternatively they may wish to include the staff who deliver these services at SPA buildings in their training needs analysis and provide them with induction training.	High	Any contractor that has access to SPA IT systems receives an induction. This recommendation relates to cleaning and security staff and SPA does not agree that it is proportionate to provide training to contractors who have no access to personal data or IT systems.
C17	Although informal follow up processes are in place these are not documented in any policy, procedure or relevant job description. Additionally, the IMT do not have the access rights to update all staff training records on SCOPE which causes problems with recording/monitoring training completion.	SPA should ensure that follow up responsibilities are documented in relevant policies, procedures and job descriptions, including those of the IMS/DPO, Line Managers and Operations Managers. To simplify the follow up process, the IMT should have appropriate access to staff training records.	High	Whilst SPA corporate do not have access to scope to update records this function is provided by Police Scotland and Forensics who can provide monitoring information.

Recommendations to close *(continued)*

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
C6	Responsibility for managing and co-ordinating IG training across the organisation has been assigned to the IG Forum and not to the individual roles involved. The IMT and the Head of Strategy and Business (HSB) (forensics) are members of the IG Forum and perform these tasks, but responsibilities are not documented in individual job descriptions.	SPA should ensure that responsibilities for managing and co-ordinating the IG training programme are documented in the job descriptions of the roles involved, namely the IMS/DPO, RMIMC and HSB.	Medium	Job descriptions for IMS and RMIMC include references to providing training. The HSB role is not expected to deliver training and inclusion in their job description is not considered appropriate.
C10	SPA's DPO oversees the induction content for both SPA and forensics' staff however it was reported that the information assurance handbook still forms part of the induction for forensics despite the DPO stating it should not be used in this way.	SPA should ensure that forensics use the information assurance handbook as an aide memoire as intended by the DPO and not as part of the induction training programme.	Medium	The Handbook was withdrawn and should not be used at all. This has been re-iterated to staff with the document removed from the network. There are compliant information management policies and procedures in place.
C12	SPA plan to deliver refresher training to all staff on an annual basis. However the lack of a training strategy/plan and formal TNA means that ICO auditors were unable to gain assurance of how appropriate refresher training would be delivered to all grades. Additionally, there is currently no requirement for staff employed by third party providers to undergo refresher data protection training appropriate to their role.	SPA should complete their TNA and training strategy/plan for next year to ensure that all staff including senior managers, forensics and those employed by third party providers receive appropriate refresher training.	Medium	*This recommendation relates to SPA Corporate only.* SPA already provides refresher IM training and no staff outside of the SPA's IM function have access to data that would require a level of training beyond that which is delivered already. IM staff are trained Data Protection Officers as evidenced during audit.
C23	Q pulse is used in the forensics department to monitor the fact that staff have read and understood policies and other documents. There are plans to introduce Q Pulse for SPA corporate staff but at the time of the audit this was not yet in place.	SPA should implement a process to provide assurance that all staff have read and understood the IG policies in place, including any updates.	Medium	The use of the Q Pulse system is considered best practice and is particularly useful for managing large staff groups. For SPA corporate staff have been asked to sign a document to confirm they have read and understood key policies.

Recommendations to close *(continued)*

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
B2	SPA do not undertake training needs analysis to identify roles that would benefit from specific training in relation to data sharing.	SPA should undertake a training needs analysis to identify roles that involve the sharing of data or involvement in ad hoc disclosures and consider what additional training may be required. Consideration should also be given to how regularly such training will need to be refreshed.	Medium	In SPA corporate there are no applicable posts involved in these processes and within Forensic Services training needs analysis is undertaken.
B11	The DSAs that were reviewed contained details of agreed retention periods; they generally consisted of setting out that the sharing partner would retain the data in line with their own retention policy. There was no indication that assurances would be sought to confirm that shared data was being disposed of in line with agreed retention periods.	SPA's DSA review process should include seeking confirmation that shared data continues to be held in adherence with the agreed retention periods and, where appropriate, that data has been disposed of.	Medium	All our data sharing is between data controllers. Each controller is responsible in their own right for how they retain and dispose of data. The SPA does not consider that it is our role or legal responsibility to seek confirmation of partners retention periods and their compliance.
B10	The DSAs that were reviewed contained details of agreed retention periods; they generally consisted of setting out that the sharing partner would retain the data in line with their own retention policy. There was no indication that checks had been undertaken to ensure that these were appropriate.	SPA's Data Sharing SOPs should be updated to include a requirement for SPA to satisfy themselves that retention periods appear appropriate.	Low	
B1	SPA's Data Sharing Standard Operating Procedures (SOPs) state that sharing decisions should be recorded in an auditable format; however, it was not clear if this was being monitored.	SPA should implement monitoring processes to ensure that the Data Sharing SOPs are being adhered to in relation to audit trails being maintained.	Low	This recommendation would apply to Police Scotland but is not considered applicable to the SPA. The SPA's data sharing is primarily legislative and within Government/ other data controllers. All current data sharing decision are made by the IM lead with records maintained.

Recommendations outstanding

This provides further detail on outstanding recommendations and revised implementation dates.

Recommendations outstanding

The follow table summarises recommendations that remain outstanding and the SPA's current plans to address the finding.

There are a number of recommendations that have now been grouped or are similar and will be achieved by a specific action. In addition, there are some actions where closure of the recommendation is reliant on Police Scotland.

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
A27	**a**) Purchases of IT related services and supplies with values below the public procurement threshold are not subject to formal contracts. **b**) SPA has no contract in place with PSoS who provide all SPA IT and Procurement services.	**a**) Whilst the public procurement thresholds may serve as a guide for whether a contract (including information security requirements) is required, there must be a process of consideration. SPA may find that in some circumstances, low value purchases will still have high risk factors and thus should be protected by contracts. **b**) SPA must address the lack of contract with PSoS, as the lack of contract provides no assurances that the services provided will continue to take place or the quality they will be provided at.	**Urgent**	a) Complete – the procurement manual requires that all IT purchases (including low value) are undertaken through the Police Scotland IT department. This allows consideration of risk factors even if a contract is not required. b) Outstanding – a draft S83 agreement has been prepared by SPA and is currently being examined with PSoS. *Reliance on Police Scotland.* *Revised due date: end of Q2 2021/22*
A28	**a**) Risk ID004 states that security clauses are not in place for all 3rd party contracts. **b**) SPA has no Service Level Agreements (SLA) in place with the PSoS IT Team.	**a**) The Risk Register shows that there is a plan in place to remedy this, with a scheduled completion by the end of the Calendar year. SPA should monitor this to ensure that completion is achieved. **b**) As the PSoS IT Team are the provider of all IT services for SPA, it is important that SPA obtain a SLA with regards to response times and communication levels.	**Urgent**	a) A security aspect letter is in place. b) As above, an s83 agreement is in progress that will include PSoS IT services. *Reliance on Police Scotland.* *Revised due date: end of Q2 2021/22*
C4	SPA do not have an IG training strategy or plan in place at present but plan to introduce one once the TNA has been completed.	SPA should ensure that a training plan or strategy is in place to ensure that training needs identified in the TNA process are addressed. The plan should document agreed timescales for delivery and responsibilities should be documented in the ToR of relevant steering groups and job descriptions.	High	Recommendation relates to SPA Corporate. A general TNA will be undertaken as part of SPA 2020. This will incorporate any information governance training requirements. However, training needs are already addressed as part of employees annual objective setting / PDR conversations. *Due date: Q1 2021/22*

Recommendations outstanding *(continued)*

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
Recommendations related to training				
C2	The information security e-learning for staff working in forensics is out of date and refers to the DPA 1998. The IMT are currently updating the content to include GDPR/DPA18 requirements. It was also reported that forensics' staff required more detailed records management training and it had already been identified that the e-learning content was not sufficient.	The information security e-learning completed by forensics' staff should be updated to reflect current data protection legislative requirements. SPA should also review and improve the records management training for forensics' staff to ensure that they are aware of their records management responsibilities.	High	The training has been updated using the Moodle eLearning platform and is waiting on being launched by Police Scotland training department. This will include an assessment and will be mandatory for all staff with compliance monitored and SCOPE records updated upon completion. *Due date: June 2021*
C8	The induction training provided to SPA corporate staff does not include an assessment or test to provide assurance that the content has been understood. It is however delivered in face to face format with an opportunity for participants to ask questions before access to systems is granted. Forensics have a test as part of the information security Moodle that staff complete. It is recommended that this is completed within the first two weeks of employment but this is not a requirement before access is granted.	**a**) SPA should ensure that data protection/information security induction training includes an assessment or test with a minimum pass rate (e.g. 80%) to ensure new staff are aware of and understand their responsibilities with respect to the handling of personal data. **b**) It should be mandatory for all staff to complete their induction as soon as possible, ideally before access is granted to systems processing personal data.	Medium	
C19	It was reported that the target for training completion was 100% allowing for long term absence however email evidence has been provided suggesting this is 90%.	SPA should consider setting KPIs or targets for training completion and documenting this in their training strategy or plan. This will assist in ensuring the effective monitoring of completion of training by staff across all departments.	Low	

Recommendations outstanding *(continued)*

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
Recommendations related to asset registers				
A5	The Hardware Asset Register is currently maintained in a form which prevents SPA from having regular access, and from being able to gain assurance that the register is kept up to date and accurate.	It was identified during the audit that there is an ongoing project to improve the Hardware Asset Register used by Police Service of Scotland (PSoS) in relation to SPA. This project should continue as planned, and SPA should ensure that assets which they rely on are tracked sufficiently to give SPA assurance of their security.	Medium	Police Scotland provides the SPA's ICT service including the ICT asset register. A project is ongoing to fully build the SPA's IT asset register which will identify the asset owner. *Reliance on Police Scotland to deliver.* *Revised due date: discussion ongoing with PS ICT department*
A6	The Software Asset Register is currently maintained in a form which prevents SPA from having regular access, and from being able to gain assurance that the register is kept up to date and accurate.	It was identified during the audit that there is an ongoing project to improve the Software Asset Register used by PSoS in relation to SPA. This project should continue as planned, and SPA should ensure that assets which they rely on are tracked sufficiently to give SPA assurance of their security.	Medium	
A7	Asset owners and security classifications are not currently tracked on the asset registers in use.	SPA should ensure that as the asset register project continues to develop, the identity of the asset owner and the relevant security classification of each asset is recorded.	Medium	
A8	No risk assessments are carried out on the existing hardware and software asset registers.	Risk assessments should be built into the new asset register as it is developed by SPA.	Medium	Recommendation rely on firstly have a complete asset register in place. After this point SPA will be able to consider risk assessment and physical checks. *Revised due date: TBC – dependent on above date.*
A9	No physical checks are carried out on the existing Hardware and Software Asset Registers.	As the new Asset Registers are developed, SPA should ensure that there is a process built in to carry out regular physical checks of their accuracy.	Medium	

Recommendations outstanding *(continued)*

Ref	Non-conformity	ICO recommendation	ICO rating	SPA update
Recommendations related to auditing				
A29	There is no review, monitoring, or auditing of existing contracts with regards to their security arrangements.	SPA have identified that this will be part of the role of new Auditor, and will take place after that role is filled. SPA should ensure that contract reviews and audits are built into the SPA Internal Audit Schedule.	Medium	These recommendations relates to different forms of auditing of security arrangements. i. Security contracts; ii. Compliance with security controls (IS020001); iii. Compliance review (eg clear desk policy / wearing ID, etc); iv. Disclosure to third parties compliance (eg to lawyers). The SPA IM team currently does not have the resources to undertake these audits. The SPA will be reviewing the staff resources required to service SPA corporate and Forensics. *Revised due date: Q1 plan; Q4 implementation.*
A37	SPA have not been carrying out a programme of internal audits of their information security.	SPA should ensure that, after filling their vacancy for an Auditor, their Internal Audit Plan includes reviews of the information security management system. This should include reviews of the IT Health Checks currently being carried out, and also of the Technical Audits done by PSoS IT.	Medium	
A38	Outside of the Forensic Services ISO 17025 requirements, there is no formalised approach to management led compliance reviews such as spot checks.	SPA should consider building into the Information Security Policy a requirement for management led compliance reviews, such as spot checks and staff surveys.	Medium	
B14	The Forensic Services Quality Team has undertaken an audit of the Defence Access process; however there was no evidence of similar quality checks or monitoring of disclosures carried out in other areas.	Regular audits or spot checks should be undertaken to provide SPA with assurance that disclosures are being made appropriately and in line with agreed policies and procedures.	Medium	