Police Service of Scotland

Data protection audit report

Auditors: [redacted]

Data controller contacts: [redacted]

Distribution:

Date of first draft:	1 July 2016
Date of second draft:	22 July 2016
Date of final draft:	09 September 2016
Date issued:	**09 September 2016**

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

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

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

Contents

1. Background

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

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

1.3 Police Service of Scotland (PSoS) has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 A conference call was held on 2 March 2016 with representatives of PSoS to identify and discuss the scope of the audit and to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with PSoS, it was agreed that the audit would focus on the following area:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

3. Audit opinion

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

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited Assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.

4. Summary of audit findings

4.1 Areas of good practice

- Information Assurance Officers provide an internal audit service to PSoS. Monthly Police National Database (PND) user audits are carried out to ensure searches are carried out for policing purpose and is reported to the Information Assurance Manager (IAM) and Regional User Group. Internal audits are documented in the Information Management Team (IMT) business plan.

- The IMT maintains a register of all the information sharing protocols (ISP), both legacy agreements and new agreements, which are in place or are in draft. The register captures the date they were signed by all relevant parties and came into force.

- Risk registers are in place to record and manage information related risks. PSoS take a three tiered approach, with risks being escalated and deescalated as appropriate between 34 different Divisional (local) registers, three Portfolio registers (DCC level), and the Corporate risk register.

4.2 Areas for improvement

- The majority of information management policies and standard operating procedures (SOPs) reviewed are outdated. The review dates noted on the coversheets of policies and SOPs suggest that the documents should have been reviewed in 2013-14. A risk assessment of all policies and SOPs was carried out and, as a result, the review cycle for information management policies and SOPs is now biennial or triennial.

- Apart from the Corporate Governance Board (CGB), there are no other steering groups, committees or equivalent, to discuss data protection related matters at a lower level to consider the items that require escalating to the CGB.

- The completion of data protection training is not monitored and completion statistics are not reported to the CGB or a steering group. There is no annual appraisal process therefore, individuals' training progression and development is not formally recorded or reported.

- The PSoS does not have an Information Asset Register (IAR) in place.

- There is no requirement to conduct Privacy Impact Assessments for new projects or for projects that involve significant changes.

5. Audit approach

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

5.2 The audit field work was undertaken at PSoS offices in Edinburgh between 14 and 15 June 2016.

6. Audit grading

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

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

7. Detailed findings and action plan

7.1 **Scope: Data Protection Governance** – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the Data Protection Act 1998 resulting in regulatory action and/or reputational damage.

Part A – Policies and Procedures, Management Structures, and Compliance and Assurance

Policies and Procedures

a1. The PSoS has a suite of data protection related policies and procedures. PSoS policies are a statement of strategic intent and the SOPs, which sit underneath the policies, provide guidance, information and instruction to Police Officers and staff members.

a2. An information management policy framework has been developed which details the information management related policies and SOPs. It was reported that the Information Management Team (IMT) have been working towards implementing the framework to ensure consistency of policies and SOPs across PSoS.

Recommendation: Continue to review policies and SOPs and work towards the information management policy framework to ensure policies and SOPs are consistent across PSoS.

Management response: Accepted. This activity is already ongoing, as noted above.
Owner: Head of Information Management
Date for implementation: In accordance with the current review timetable set by Policy Support.

a3. Policies and SOPs are drafted by owners within relevant business areas. Once drafted, a data protection compliance check and equality impact assessment (EIA) is carried out.

a4. Policies and SOPs follow an agreed format, style and version control process which is documented in the Governance SOP and the Formatting Standard Guidance for Record Sets. The Policy Support team are responsible for ensuring that policies and SOPs follow the agreed standard.

a5. Administrative information is detailed on the coversheet of all policies and SOPs. The information recorded on the coversheet includes the owning department, author/reviewer, version number, date published, date of review and details of the compliance checks that have been carried out.

a6. The majority of information management policies and SOPs reviewed are outdated. The review dates noted on the coversheets of policies and SOPs suggest that the documents should have been reviewed in 2013-14. It was reported that previously policies and SOPs had an annual review period. An internal risk assessment of all policies and SOPs was carried out and, as a result, the review cycle for information management policies and SOPs is now biennial or triennial.

Recommendation: Review all information management policies and SOPs on an annual basis if possible, or every two years as a maximum, to ensure that the content remains appropriate and up-to-date.

Management response: Partially accepted. The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. This will take into account the standard applied across PSoS, the balance of work between policy review and improvement activity, and the fact that a policy or SOP can be updated at any time in response to a change to the external environment.
Owner: Head of Information Management
Date for implementation: 31 March 2017

a7. It was reported that the policy and SOP template has now changed and as a result, the information table located on the coversheet no longer records when the document is due for a review. The Governance SOP mirrors the updated template.

Recommendation: As a minimum, all policies and SOPs should clearly record the owning department, author, version number and next scheduled review date.

Management response: Rejected. The owning department and version number is already recorded on policies and SOPs. The other data elements are held by Policy Support rather than on the published document, as practice has shown that publishing information is counter-productive.
Owner: Not applicable
Date for implementation: Not applicable

a8. All policies and SOPs undergo a mandatory consultation which involves key stakeholders and trade associations. Once the consultation is completed, the Policy Support team are responsible for arranging the approval of the policy or SOP.

a9. Policy and SOP approval is documented in an approval record and signed off at Assistant Chief Constable (ACC) or Deputy Chief Constable (DCC) level. At this stage, the review date for the document is determined and noted on the approval record.

a10. A Policy and SOP tracker is maintained by the Policy Support team which details the title of the document, the owning department, responsible person, author, review notification date and review date. A number of information management policies are flagged as under review.

a11. The Policy Support team are responsible for notifying authors within business areas when a policy or SOP is due for a review.

a12. The period within which a review of policies and SOPs should be completed is 16 weeks but can be extended if necessary. This is not formally documented in a policy or SOP.

Suggestion: Consider formalising a timeframe in which a policy or SOP review should be completed within and document this in an appropriate policy or SOP. For example, the Governance SOP.

Management response: Accepted. Consideration will be given to adding the timeframe during the forthcoming review of the SOP.
Owner: Head of Policy Support
Date for implementation: In accordance with SOP review timescale

a13. There is an Information Management Policy Group (IMPG) which is responsible for reviewing the IMT's policies and SOPs. The action to review and update certain information management policies and SOPs is recorded in the IMT's business plan.

a14. It was reported that staff are notified of any new or updated policies or SOPs through a message displayed on the front page of the intranet. However, it was reported that this does not always happen in practice. In some cases, line managers may notify staff of any new or updated policies and SOPs through email.

Recommendation: Ensure that line managers notify staff directly regarding any new or updated policies and SOPs. Notifications can be disseminated in emails, divisional bulletins or newsletters.

Management response: Partially accepted. An email is already sent to all business units informing them of new publications. The content of the email has been expanded to state explicitly that business units co-ordinate onward communication through the appropriate medium.
Owner: Head of Policy Support
Date for implementation: 31 August 2016

a15. Staff are asked to sign and confirm that they will abide by relevant policies and procedures on their induction. A disclaimer is also displayed on the log on screen of PSoS computers, which asks staff to accept terms and conditions and agree to comply with relevant policies and SOPs.

Management Structures

a16. The Information Management department sits within Corporate Governance and is divided into two areas: Information Assurance (IA) and Information Disclosure (ID). The IA and ID Managers both report to the Head of Information Management (HOIM) who, in turn, reports to the Head of Corporate Governance (HOCG). The HOCG reports to the Director or Corporate Services; however the Director of Corporate Services has left PSoS and the position is currently unfilled. All Directors report to the DCC designate.

a17. The governance structure which supports data protection, records management and security management is not formally documented to clearly show reporting lines.

Recommendation: PSoS should create an organisational governance chart which clearly demonstrates the reporting lines and flows of information between groups covering information and risk management.

Management response: Partially accepted. Information governance roles and relationships will be articulated in an Information Governance SOP rather than a chart.
Owner: Head of Information Management
Date for implementation: 31 March 2017. [This takes into account the timescale to appoint a corporate director]

a18. Until recently the DCC designate was the Senior Information Risk Owner (SIRO) for PSoS; the Director of ICT has now been appointed to this role and has overall strategic responsibility for information management. It was reported that the Director of ICT's job description has not been updated to include the role and responsibilities of SIRO.

Recommendation: Formally document the role and responsibilities of the SIRO and include in the job description.

Management response: Partially accepted. Information governance roles and relationships will be articulated in an Information Governance SOP rather than in job descriptions.
Owner: Head of Information Management
Date for implementation: 31 March 2017

a19. The role of Information Asset Owners (IAOs) has recently been established and has been assigned to ACCs and Directors across PSoS.

a20. All roles and responsibilities in relation to information management are not formally documented within a policy or SOP.

Recommendation: Identify key roles and responsibilities in relation to information management and formalise by documenting these.

Management response: Accepted. Information governance roles and relationships will be articulated in an Information Governance SOP**.**
Owner: Head of Information Management
Date for implementation: 31 March 2017

a21. There is Corporate Governance Board (CGB) which is chaired by the DCC designate. Meetings are scheduled quarterly and attendees include the SIRO, Directors, ACCs, HOCG and HOIM.

a22. The role of the CGB is to ensure that PSoS is complying with legal and operational controls in relation to information management, risk and business continuity. There is a standard agenda item for the CGB which includes information management and risk management.

a23. The HOIM is responsible for reporting on information management to the CGB. Information compliance reports are submitted to the CGB every quarter and signed off. Apart from the CGB, there are no other formal mechanisms for the HOIM to report to the SIRO.

Recommendation: Create an Information Governance Steering Group which is responsible for providing general oversight for information governance and data protection compliance. This would allow key roles to report and discuss any data protection concerns and identify what concerns will need to be included in the information compliance report and escalated to the CGB.

Management response: Accepted. This will form part of the strengthened information governance regime set out in the Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

a24. The CGB has an action log in place to record outstanding actions. The log documents a description of the action and owner. Actions are discussed at the beginning of each CGB meeting.

a25. The CGB provides the internal assurance forum in PSoS. Information risk is also reported to the quarterly Audit and Risk Committee of the Scottish Police Authority (SPA). The DCC Designate, Directors and HOCG attend the committee to report on information compliance.

a26. It was reported by the SIRO that there is a Senior Leadership Board (SLB) which is chaired by the Chief Constable (CC). It was reported that there is a standard agenda item for the SLB which includes information assurance; however, the SIRO was unsure if this is still an agenda item following recent changes. The HOIM was uncertain if SLB meetings still occurred. No up-to-date meeting minutes were provided to confirm that the SLB still exists.

Recommendation: a) Ensure information assurance is included as a standard agenda item for the SLB to discuss.

b) Please refer to recommendation at **a17**.

Management response: Rejected. The Force Governance Board (formerly Corporate Governance Board) is the means by which the Executive exercises oversight of information assurance. This is a standing agenda item, and fits with the Board's remit for risk management, audit activity and business continuity.
Owner: Not applicable
Date for implementation: Not applicable

a27. There is currently no staff forum in place to facilitate operational staff raising data protection queries or issues. Where advice on such matters is required, it was reported that staff would contact the IMT directly.

Recommendation: Introduce mechanisms that would enable staff to raise data protection concerns or queries. Any issues raised should be discussed and escalated where necessary.

Management response: Rejected. A staff forum is impractical given the size and geographical spread of Police Scotland. The mechanisms currently in place to enable staff to raise data protection issues (dedicated IA team, monitored group mailbox, visible intranet presence and clear ownership of information assurance policies and procedures) are considered sufficient.
Owner: Not applicable
Date for implementation: Not applicable

Compliance and Assurance

a28. PSoS audit service providers are both external and internal. The external audit service is provided by Scott Moncrieff who are instructed to carry out audits of PSoS by the Audit and Risk Committee which is overseen by the SPA.

a29. An information management audit has not yet been completed by the external provider. It was reported that Scott Moncrieff has been instructed by the Audit and Risk Committee to carry out an audit this year; it will focus on information management and security. The internal audit assignment plan details the purpose of the audit.

a30. Information Assurance Officers are responsible for delivering an internal audit service for PSoS. Audits to be carried out are documented in the IMT's business plan. Completed and on-going audits include an audit of unencrypted devices, destruction arrangements and technical security.

a31. PND user audits are carried out, on a monthly basis, on one percent of the searches conducted on the system. The PND user audit involves checking access to systems and

ensuring that a search has been conducted for a legitimate policing purpose. This involves contacting the Supervisor of the Police Officer in question to seek confirmation.

a32. A report is produced detailing the outcomes of the PND user audit. This is reported to the IAM and Regional User Group (RUG). The RUG meeting is held every six months and is chaired by the Superintendent.

a33. The business area that the audits relate to is responsible for implementing any recommendations that are made. The Information Assurance Officer is responsible for tracking the business area's progress. There is no central plan which pulls together the recommendations of internal and external audit service providers.

Recommendation: Create a central plan which records the recommendations of internal and external audit service providers to identify key areas of concern, plan solutions and monitor improvements.

Management response: Accepted. A tracker for all audit and inspection activity will be maintained for the Force Governance Board.
Owner: Head of Corporate Governance
Date for implementation: 31 December 2016

a34. It was reported by the HOIM that there are a number of standards that PSoS are required to meet. These derive from the HMG SPF, Codes of connection for PSN and the Public Records Act requirements. The SIRO also reported that PSoS self-assess against the ISO27001 information security standards; however, no evidence was provided to support this comment.

a35. As previously mentioned, HOIM is responsible for producing information compliance and security reports which provides an insight into organisational performance. There does not appear to be any overarching key performance indicators (KPI) in place for data protection.

Recommendation: The PSoS should create and utilise KPIs to assist in monitoring performance against compliance with the Data Protection Act (DPA).

Management response: Accepted. KPIs for training, information sharing and subject access will be monitored by the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

Part B – Training and Awareness and Data Sharing

Training and Awareness - Management Structures

b1. The data protection SOP states that all staff will receive data protection training as part of their induction process and that access to the IT network and systems will not be permitted until appropriate training has taken place. The SOP gives a high level indication of the topics that should be covered in the training.

Recommendation: PSoS should develop a stand-alone SOP for data protection training to provide further detail and context of the necessary requirements of a data protection training programme in a police context.

Management response: Partially accepted. The PSoS approach to data protection training will be documented in a design specification with lesson plans, as is the case with all training inputs.
Owner: Head of Training Delivery

Date for implementation: 31 March 2017

b2. The Information Security SOP also includes a section on training and awareness which states that all staff must undergo regular security awareness training, to ensure that staff are aware of their responsibilities in relation to information security to allow them to carry out their duties in a secure manner.

b3. It was reported that PSoS has a specialist overall Learning & Development Division which oversees and coordinates training for all civilian staff and Police Officers/Special Constables.

b4. Subject matter experts within each division have responsibility for the actual delivery of data protection training. Police Officers and Special Constables will receive their training as part of their induction course at the PSoS College of Policing.

b5. It was reported that all PSoS training sessions should be subject to a bi-annual review against the National Quality Assurance Training Standards; however, PSoS were unable to confirm when the last review had taken place.

Recommendation: PSoS should ensure that all training modules are assessed in line with the requirements of the National Quality Assurance Training Standards.

Management response: Accepted. Data Protection training will be reviewed in line with the National Framework for Quality Assurance in Training and Education.
Owner: Head of Quality Assurance
Date for implementation: Continuous review

b6. PSoS are due to launch a new overall training strategy and accompanying strategic committee on training and development in August 2016. This committee will deal with all aspects of training with a much greater scope than data protection.

Recommendation: The creation of an IG Steering Group would allow PSoS to specifically discuss data protection and information security training requirements. Once data protection training needs have been identified, the IG steering group can report back to the training committee. Please refer to recommendation **a23** regarding the creation of an IG Steering Group.

Management response: Accepted. Information management training will constitute a standing item for the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b7. It was reported that a new training identification process and form is being developed to allow Divisions to identify training needs and apply for resource to deliver that training. There was no indication given as to when this might be in place.

Recommendation: PSoS should implement this process as soon as is practicable and ensure that relevant staff across PSoS are made aware of the process.

Management response: Partially accepted. The Information Governance Steering Group will be responsible for ensuring a coherent programme of data protection training and awareness is in place. The training identification process will be a supplementary means by which training needs can be identified and processed.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b8. A number of IMT staff have the requirement to either develop or deliver formal training on data protection and information security standards to Police Officers and staff. This responsibility is included in their job descriptions. However, it was reported that subject matter experts in other areas of PSoS deliver similar training, potentially leading to an unnecessary duplication of effort.

Recommendation: The responsibilities of subject matter experts and of IMT staff should be clarified to avoid the duplication of effort in the delivery of data protection training.

Management response: Partially accepted. The deployment of different officers and staff to undertake induction training, post-specific training and in-service awareness is considered to be an effective approach to training during an officer or member of staff's service. Nevertheless the responsibilities will be documented and potential overlaps subject to resolution by the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b9. Specialist training on data protection and other associated training is provided on a role-based and at the time of need basis. Staff in the IMT have attended a number of training courses over the last 6 months; however, it was unclear if there was a specific plan or training needs analysis around this activity.

Recommendation: A training plan should be put in place that details the training requirements for all specialist data protection roles and the timescales in which they should be delivered from the start of employment.

Management response: Rejected. The role profile for each role already specifies the level of knowledge and skill required, and PSoS will use the performance assessment methods to plan training requirements for individual members of staff.
Owner: Not applicable
Date for implementation: Not applicable

b10. Training on data protection offences is delivered, by the Counter Corruption Unit (CCU), to Police Officers and Special Constables. This training package was driven by the CCU's own initiative and is not connected to a wider PSoS training plan or strategy.

Recommendation: Please refer to recommendation at **b1**.

Management response: Please refer to recommendation at **b1**.
Owner: Please refer to recommendation at **b1**.
Date for implementation: Please refer to recommendation at **b1**.

Training and Awareness – Monitoring and Reporting

b11. PSoS has software in place to record the completion of training by Police Officers and staff, but training completion rates are not being requested from any area of PSoS nor collated.

b12. Training completion statistics are not currently presented to the CGB and there is no discussion on training and awareness.

Recommendation: Completion level statistics for data protection training should be reported to the IG Steering Group (please refer to recommendation at **a23**) and if necessary, escalated to the CGB. Relevant training and

awareness KPIs and targets should also be created and monitored as appropriate.

Management response: Partially accepted. Information management training will constitute a standing item for the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b13. There is no annual appraisal process being undertaken within PSoS, so individuals' training progression and development are not being formally recorded and reported. It was reported that staff performance and training needs are assessed as part of routine tasking and line management activities.

Recommendation: The annual appraisal process should be restarted within the IMT so there can be an accurate assessment of individual staff acquired skills and ongoing development needs in regards to data protection.

Management response: Rejected. IMT staff will be subject to any appraisal process agreed with staff side associations for implementation across the Service. In the meantime, current performance assessment methods will be used.
Owner: not applicable
Date for implementation: not applicable

b14. The CCU does present the relevant Divisional Commander with a brief post-training report to indicate levels of attendance of the session and any relevant feedback from officers.

Data Sharing – Informed Decision Making

b15. There is an Information Sharing SOP which was published in October 2013. The SOP is outdated and it was reported that the SOP is currently under review.

Recommendation: The Information Sharing SOP should be reviewed on an annual basis to ensure it remains up to date and in line with current practice. Please refer to recommendation at **a6**.

Management response: Partially accepted. The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b16. The Information Sharing SOP details the common legal gateways for sharing, the requirement to produce an information sharing protocol for regular data sharing and roles and responsibilities of the Divisional Commander and IMT.

b17. The IMT maintains a register of all the information sharing protocols (ISP), both legacy agreements and new agreements, which are in place or are in draft. The register captures the date they were signed by all relevant parties and when they came into force.

b18. The IMT are in the process of building a library of ISP templates for relevant areas of PSoS to use as a basis for their drafts; this is intended to ensure that agreements are as clear and consistent as possible before they go through compliance checks. Evidence has been provided of a number of templates already in place.

b19. All new ISPs will be reviewed six months after implementation, to ensure that they are operating as intended, and every 3 years thereafter, unless there is a

significant change in legislation or in the data sharing process.

b20. One-off disclosure activity is governed by two SOPs, one for Public Interest Disclosures and the other for Requests for Personal Information from External Bodies.

b21. The SOPs detail the purposes for which PSoS can disclose information, how to reach decisions on disclosures and the processes and practicalities around disclosures.

b22. PSoS acknowledged during the audit that it is unlikely that the Requests for Personal Information from External Bodies SOP, or the 'Section 29' process as it is known internally, is being applied properly by some business areas. It was reported that the IMT will be undertaking an audit to assess the application of the Section 29 SOP across PSoS in the second half of 2016.

Recommendation: This audit activity should be completed as soon as is practicable and any recommendations implemented to ensure consistency and compliance in the use of the 'Section 29' process across PSoS.

Management response: Accepted. This activity is already ongoing, as noted in the report.
Owner: Head of Information Management
Date for implementation: 31 December 2016

b23. PSoS are in the process of setting up Risk & Compliance Hubs in each Division. The Hubs will seek to provide specialist training to operational staff on the requirements of data sharing in order to comply with the requirements of the Named Persons Service, which is due to come into force in Scotland in August 2016.

b24. Significant data sharing risks or concerns are reported to the CGB by the HOIM. There is no other group or committee to discuss data sharing risks or queries at a local level.

Recommendation: Data sharing should be added as a standard agenda item for the IG Steering group to discuss any risks or concerns relating to current data sharing projects. Any risks identified should be reported to the CGB if necessary. Please refer to recommendation **a23** regarding the creation of an IG Steering Group.

Management response: Partially accepted. Information sharing will constitute a standing item for the Information Governance Steering Group. Information Management will continue to gather information about information sharing project risks and concerns through Organisational Development**.**
Owner: Head of Information Management
Date for implementation: 31 March 2017

Data Sharing – Assessing Legality, Risks and Benefits

b25. There is no policy or SOP in place which requires a Privacy Impact Assessment (PIA) to be conducted for new projects in which, personal data is shared or for existing projects where a significant change is involved. The Information Sharing SOP includes a PIA in the flowchart of actions for new data sharing arrangements, but does not make it mandatory.

Recommendation: The requirement to conduct a PIA for all new projects, including projects involving data sharing, should be documented in a policy or SOP. The policy or SOP should set out a clear process for determining when a PIA should be conducted, who it will be authorised by, how it will be incorporated into the project plan and how compliance

will be monitored. The policy or SOP should clearly identify the roles responsible for completing PIAs.

Management response: Partially accepted. The requirement to conduct a PIA in certain circumstances will be set out in an appropriate Police Scotland standard operating procedure.
Owner: Head of Information Management
Date for implementation: 31 March 2017

b26. It was reported that a project board is created for major projects that the PSoS are involved in. There is a representative from the IMT on the project board, who are responsible for producing a brief report at the beginning of the project, to provide advice on what PSoS is required to consider in regards to data protection, records management and information security.

b27. At the final stages of a project, the IMT representative will also contribute to the project board's risk report with any outstanding data protection risks that are still a concern before the final decision to proceed. The board will then have to make a decision as to whether to accept or mitigate the identified risk(s).

b28. It was reported that for smaller projects, the IMT are responsible for conducting a compliance check on the proposed project.

Part C - Information Risk Management and Security

Information Risk Management

c1. There is a Risk Management SOP which sets out how the organisation manages risk in general. The SOP does not specifically mention information risk.

Recommendation: PSoS should introduce an Information Risk Strategy to set out how the organisation will manage information risk specifically.

Management response: Partially accepted. The manner in which PSoS manages information risk will be articulated in the Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c2. Operational responsibility for risk sits with the HOCG, who is also the Head of Risk and Business Assurance. The Risk Team consists of two Risk Management Officers (RMO).

c3. Risk registers are in place to record and manage information-related risks. PSoS take a three tiered approach, with risks being escalated and de-escalated, as appropriate, between 34 different Divisional (local) registers, 3 Portfolio registers (DCC level), and the corporate risk register.

c4. Information-related risks are not recorded separately from the main risk registers; however, it was reported that RMOs liaise with the HOIM regarding information risks where necessary.

Suggestion: It would be good practice to also introduce a separate risk register specifically for information risks to ensure adequate oversight and mitigation of these risks.

Management response: Rejected. PSoS consider it is important to manage information risk alongside other risks facing the Service to ensure a consistent approach to the assessment, mitigation, reporting and scrutiny of risk.
Owner: Not applicable
Date for implementation: Not applicable

c5. The corporate risk register and portfolio risk registers are reported by the HOCG to the quarterly CGB to ensure board level oversight.

c6. Corporate risks are approved by the CGB and it was reported that the DCC challenges the HOCG on the progress of risks.

c7. There is no risk subcommittee, steering group or equivalent in place which considers the escalation of information risk to Board level. It was reported that department heads are responsible for oversight of local registers and escalation of risks where appropriate. The main mechanism for discussing information risks is the CGB.

Recommendation: Risks can be discussed at a lower level at the IG Steering Group (recommendation at **a23**) to consider the risks that require escalating to the CGB. The IG Steering Group should report on the information risk strategy recommended at **c1** and provide oversight of the information risk register recommended at **c4**.

Management response: Accepted. Information risk will constitute a standing item for the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c8. The SIRO is responsible for information risk within PSoS. Due to lack of availability, the SIRO has not yet been able to undertake SIRO training, though training has been booked for August.

Recommendation: The SIRO should have relevant training as soon as practicable to ensure that he is fully aware of his role and responsibilities. This should also be formally recorded in his job description. Please refer to recommendation at **a18**.

Management response: Accepted. The SIRO has completed a training course.
Owner: Director of ICT
Date for implementation: 31 August 2016

c9. The SIRO reported that he has a good understanding of the SIRO role from previous private sector responsibilities where he acted as Certified Information Security Manager (CISM) and default Data Protection Officer (DPO).

c10. As previously mentioned, the SIRO attends the CGB in his capacity as the SIRO, Director of ICT and IAO for information relating to ICT.

Recommendation: In order to obtain adequate oversight and assurance, it would be good practice for the SIRO to not carry out separate roles, such as IAO, which may overlap with his SIRO responsibilities.

Management response: Partially accepted. The information governance framework already in place separates the roles of SIRO and IAO. The policy will be reviewed on appointment of a corporate director.

Owner: Head of Information Management
Date for implementation: 31 March 2017

c11. As previously mentioned, the role of IAO has been established at ACC and Director level. IAOs have received specialised information risk training from a third party provider, in 2015. Refresher training has not been provided to IAOs due to staff changes, which has resulted in IAOs leaving their role. Some IAOs have not yet been replaced. It was unclear whether IAO responsibilities are recorded in job descriptions.

Recommendation: IAOs should receive training on a regular basis to ensure that they are aware of their roles and responsibilities. PSoS should provide training to new and existing IAOs as soon as practicable. PSoS should ensure that these responsibilities are also formally documented in job descriptions.

Management response: Partially accepted. Information governance roles and relationships will be articulated in an Information Governance SOP, rather than in job descriptions. Training will be provided to IAOs on approval of the Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c12. IAOs currently each have a large portfolio due to their grade. It was reported that, in reality, IAOs act at a strategic level whereas Operational Business Owners carry out the more operational aspects of the IAO role. However, this is not formally documented.

Recommendation: Operational Business Owners responsible for carrying out the operational aspects of the IAO role should be appointed as Information Asset Administrators (IAA). Formally document the roles of IAAs and IAOs to ensure that all information assets are being appropriately managed.

Management response: Accepted. Information governance roles and relationships will be articulated in an Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c13. There is currently no IAO forum or equivalent for IAOs to discuss relevant issues and report to the SIRO.

Recommendation: PSoS should introduce a forum for IAOs to regularly meet with the SIRO and discuss issues relating to their role. Alternatively, IAOs can discuss relevant issues or concerns at the IG Steering Group (Please refer to recommendation at **a23**).

Management response: Rejected. PSoS considers that the Force Governance Board, the proposed Information Governance Steering Group and the establishment of formal reporting to the SIRO provide sufficient engagement opportunities to raise information governance issues.
Owner: Not applicable
Date for implementation: Not applicable

c14. PSoS does not have an Information Asset Register (IAR) in place, although they have compiled a high level register documenting IAOs. This register does not include specific information assets but instead sets out who each IAO is for particular business areas. The HOIM and the IA Manager have been working on developing a more comprehensive IAR.

Recommendation: a) PSoS should introduce a comprehensive IAR containing all information assets including paper records. This should also identify IAOs for

each asset and document the outcomes of periodic risk assessments of assets to ensure that the data held by each information system is controlled and kept securely.

b) PSoS should assign overall responsibility for maintaining the new IAR to an appropriate staff member and ensure that all policies and procedures that mention the IAR, such as the IT Systems Development SOP, are updated accordingly.

Management response: Accepted. The creation and maintenance of a detailed information asset register will be the responsibility of the Records Manager.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c15. IAOs are responsible for maintaining, regularly reviewing and reporting on their local risk registers. It was reported that there is no standard route for IAOs to provide assurance to the SIRO and there is no SOP providing guidance for IAOs.

Recommendation: PSoS should introduce formal IAO reporting to the SIRO on a regular basis, for example, through the suggested IAO forum or through the IG Steering Group. This would ensure that all information assets are regularly risk assessed, and that the SIRO has appropriate oversight of how these risks are being managed.

Management response: Partially accepted. Information governance roles and relationships, including formal reporting relationships, will be articulated in an Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c16. Similar to data sharing, PIAs are not required to be conducted for all new or significant changes to ICT systems processing or storing personal data. It was reported that the IA team are informed of all new projects and that EIAs consider some elements of PIAs.

Recommendation: Please refer to recommendation at **b25** regarding the requirement to undertake PIAs.

Management response: Partially accepted. Please refer to recommendation at b25.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c17. Evidence was provided to auditors to support that a PIA had been conducted for the Stop and Search project in 2013; however, whilst a PIA was conducted on this project, PIAs, are not undertaken routinely by PSoS. The Stop and Search PIA included, amongst other things, background on the wider legislation around privacy, details of the privacy risks identified and the solutions to mitigate the risks.

Recommendation: PSoS should consider basing any future PIA template on the PIA that was used for the 'Stop and Search' Project in 2013. As a minimum, PIAs should include a consultation process with the IMT and detail the results of the PIA including the proposed information flows, compliance risks and mitigating risks. You may wish to refer to our PIA Code of Practice for further guidance.

Management response: Partially accepted. The methodology for conducting a PIA will be set out in an appropriate PSoS SOP. Completed PIAs will be used by the IA team as exemplars.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c18. PSoS has a Security Incident Reporting and Management SOP which was due to be updated in June 2014. This states that the HOIM should be informed of all information security incidents. It also states that the HOIM, in consultation with the relevant IAO, will assess the risks associated with the incident.

c19. The HOIM reports to the CGB on security incidents for the quarter, including near misses, and details of mitigation measures undertaken as a result.

c20. Although incident analysis and risk assessments of information assets feed into risk management structures, it is unclear whether risks identified as part of any PIAs currently undertaken by PSoS also feed into the organisation's risk management structures. There is therefore a risk that PSoS are not appropriately managing all identified risks.

Recommendation: PSoS should ensure that risks identified via PIAs, as well as those identified through incident analysis and risk assessments of information assets, feed into the organisation's risk management structures and are escalated appropriately. The PIA SOP recommended above should stipulate that this happens.

Management response: Partially accepted. The manner in which PSoS manages information risk will be articulated in the Information Governance SOP.
Owner: Head of Information Management
Date for implementation: 31 March 2017

Security – Policy - Management Direction

c21. PSoS have an overarching Information Security policy and accompanying Information Security SOP. The SOP was published in 2013 and due for a review in 2014. The policy was published in Feb 2014 and due for a review in April 2014. As a result of the risk assessment carried out, the policy and SOP were due for a review in November 2015. It was reported that the Information Security policy was being updated shortly after the audit site visit. This policy and SOP are aligned with the HMG Security Policy Framework (SPF).

Recommendation: Ensure the Information Security Policy and corresponding SOP are updated and reviewed annually. Please refer to recommendation at **a6**.

Management response: Partially accepted. The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c22. PSoS have also published activity-specific SOPs which sit underneath this overarching Information Security policy such as the Email and Internet Security SOP, ICT User Access and Security SOP and the Mobile Data and Remote Working SOP. The Information Security policy and SOPs are owned by the IAO, the Director of Corporate Services. The majority of SOPs and policies provided were outdated.

Recommendation: Ensure all policies and SOPs are updated and reviewed annually. Please refer to recommendation at **a6**.

Management response: Partially accepted. The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c23. PSoS do not have a standalone information risk management policy and criteria. However, the Information

Security SOP includes reference to risk management and the Risk Management SOP is also applied to information security risks.

Recommendation: PSoS should introduce a standalone information security risk management policy to document how the organisation deals with information security risks.

Management response: Rejected. PSoS consider it is important to manage information security risk alongside other risks facing the Service to ensure a consistent approach to the assessment, mitigation, reporting and scrutiny of risk. The existing suite of SOPs for information security is considered sufficient.
Owner: Not applicable
Date for implementation: Not applicable

c24. Information security is recorded as a risk on the corporate risk register. This register is reviewed quarterly and is discussed at the CGB, in order to establish oversight of information security at an appropriate level.

c25. Where appropriate, information security policies or initiatives are supported by high level management communications. For example, in March 2016 the DCC sent a memorandum to Divisional Commanders and Department Heads reminding them of the need for all staff to comply with the Email and Internet Security SOP. It was reported that this was the result of a security incident.

Security – Policy- Internal Organisation

c26. The Information Security SOP includes a section on roles and responsibilities in relation to information security. These are also appropriately recorded in the Information Security Manager's job description.

c27. Information security responsibilities for data processors are recorded in the template data processor agreement. It was reported that, depending upon the sensitivity of the information being processed, security requirements may be recorded in a separate but referenced agreement.

c28. Risk assessments are included with, and linked to, risk registers, as set out in the Risk Management SOP.

c29. Information security risk assessments are also conducted as part of the PSoS system accreditation process. Risk assessment and risk treatment methodologies in this regard are aligned with HMG SPF.

c30. It was reported that Risk Management and Accreditation Document Sets (RMADS) are in place for all key systems and are regularly reviewed.

c31. The ICT Systems Development SOP, which was last reviewed in 2013 and due for a review in October 2016 states that 'information must be protected from threats and vulnerabilities through full risk assessment and the implementation of appropriate controls'. Auditors were provided with evidence that risk assessments had been conducted for specific ICT systems such as PND, and in circumstances where police network access was required at a council-owned building. However, for the PND risk assessment provided the date of review field was blank, and the other did not have the option to record a review date.

Recommendation: Review and update the ICT Systems Development SOP. Please refer to recommendation at **a6**. Risk assessments should be reviewed on a regular basis to reassess the level of risk. PSoS should ensure that implemented controls still appropriately address identified risks.

Management response: Rejected. Regular review of risk controls is already an established element in the PSoS approach to risk management.
Owner: Not applicable
Date for implementation: Not applicable

c32. Risk registers clearly evidenced ownership of information risks and documented progress of risks through the inclusion of risk trends. The Corporate risk register also explicitly states whether scores have reduced, increased, or remained static compared to the previous quarter.

c33. PSoS does not have a steering group or similar to provide oversight of information security related issues.

Recommendation: Please refer to the recommendation at **a23** regarding the creation of an IG Steering Group. Information security should be included as a standard agenda item and issues escalated to the CGB, where necessary.

Management response: Accepted. Information security will constitute a standing item for the Information Governance Steering Group.
Owner: Head of Information Management
Date for implementation: 31 March 2017

c34. There is also no formal work plan for information security; however, Information Security's work is structured by PSoS projects and compliance deadlines such as for PSN Code of Connection.

Recommendation: PSoS should formally document their information security work plan in order to monitor progress with projects and compliance deadlines.

Management response: Partially accepted. A composite work plan for the IA team will enable progress with projects to be monitored.
Owner: Head of Information Management
Date for implementation: 31 March 2017

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

7.3 Any queries regarding this report should be directed to [redacted] Engagement Lead Auditor, ICO Good Practice.

7.4 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. HOIM [redacted] was particularly helpful in organising the audit.

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months Describe the status and action taken.	Progress at 6 months Describe the status and action taken.
a2. Continue to review policies and SOPs and work towards the information management policy framework to ensure policies and SOPs are consistent across PSoS.	**Management response: Accepted.** This activity is already ongoing, as noted above. **Owner:** Head of Information Management **Date for implementation:** In accordance with the current review timetable set by Policy Support.		
a6. Review all information management policies and SOPs on an annual basis if possible, or every two years as a maximum, to ensure that the content remains appropriate	**Management response: Partially accepted**. The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. This will take into account the standard applied across		

and up-to-date.	Police Scotland, the balance of work between policy review and improvement activity, and the fact that a policy or SOP can be updated at any time in response to a change to the external environment. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
a7. As a minimum, all policies and SOPs should clearly record the owning department, author, version number and next scheduled review date.	**Management response: Rejected**. The owning department and version number is already recorded on policies and SOPs. The other data elements are held by Policy Support rather than on the published document, as practice has shown that publishing information is counter-productive. **Owner:** Not applicable **Date for implementation:** Not applicable		
a12. Consider	**Management response:**		

formalising a timeframe in which a policy or SOP review should be completed within and document this in an appropriate policy or SOP. For example, the Governance SOP.	**Accepted.** Consideration will be given to adding the timeframe during the forthcoming review of the SOP. **Owner:** Head of Policy Support **Date for implementation:** in accordance with SOP review timescale		
a14. Ensure that line managers notify staff directly regarding any new or updated policies and SOPs. Notifications can be disseminated in emails, divisional bulletins or newsletters.	**Management response:** **Partially accepted.** An email is already sent to all business units informing them of new publications. The content of the email has been expanded to state explicitly that business units co-ordinate onward communication through the appropriate medium. **Owner:** Head of Policy Support **Date for implementation:** 31 August 2016		
a17. PSoS should create an organisational governance chart	**Management response:** **Partially accepted.** Information governance roles and relationships will be		

which clearly demonstrates the reporting lines and flows of information between groups covering information and risk management.	articulated in an Information Governance SOP rather than a chart. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017. [This takes into account the timescale to appoint a corporate director]		
a18. Formally document the role and responsibilities of the SIRO and include in the job description.	**Management response: Partially accepted.** Information governance roles and relationships will be articulated in an Information Governance SOP, rather than in job descriptions. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
a20. Identify key roles and responsibilities in relation to information management and formalise by documenting these.	**Management response: Accepted.** Information governance roles and relationships will be articulated in an Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
a23. Create an	**Management response:**		

Information Governance Steering Group which is responsible for providing general oversight for information governance and data protection compliance. This would allow key roles to report and discuss any data protection concerns and identify what concerns will need to be included in the information compliance report and escalated to the CGB.	**Accepted.** This will form part of the strengthened information governance regime set out in the Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
a26. Ensure information assurance is included as a standard agenda item for the SLB to discuss.	**Management response: Rejected.** The Force Governance Board (formerly Corporate Governance Board) is the means by which the Executive exercises oversight of information assurance. This is a standing agenda item, and fits with the Board's remit for risk management, audit activity and business continuity. **Owner:** Not applicable		

	Date for implementation: Not applicable		
a27. Introduce mechanisms that would enable staff to raise data protection concerns or queries. Any issues raised should be discussed and escalated where necessary.	**Management response:** **Rejected.** A staff forum is impractical given the size and geographical spread of PSoS. The mechanisms currently in place to enable staff to raise data protection issues (dedicated IA team, monitored group mailbox, visible intranet presence and clear ownership of information assurance policies and procedures) are considered sufficient. **Owner:** Not applicable **Date for implementation:** Not applicable		
a33. Create a central plan which records the recommendations of internal and external audit service providers to identify key areas of concern, plan solutions and monitor improvements.	**Management response:** **Accepted**. A tracker for all audit and inspection activity will be maintained for the Force Governance Board. **Owner:** Head of Corporate Governance **Date for implementation:** 31 December 2016		
a35. The PSoS should create and utilise KPIs	**Management response:** **Accepted.** KPIs for training,		

to assist in monitoring performance against compliance with the Data Protection Act (DPA).	information sharing and subject access will be monitored by the Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
b1. PSoS should develop a stand-alone SOP for data protection training to provide further detail and context of the necessary requirements of a data protection training programme in a police context.	**Management response:** **Partially accepted.** The PSoS approach to data protection training will be documented in a design specification with lesson plans, as is the case with all training inputs. **Owner:** Head of Training Delivery **Date for implementation:** 31 March 2017		
b5. PSoS should ensure that all training modules are assessed in line with the requirements of the National Quality Assurance Training Standards.	**Management response:** **Accepted.** Data Protection training will be reviewed in line with the National Framework for Quality Assurance in Training and Education. **Owner:** Head of Quality Assurance **Date for implementation:**		

	Continuous review		
b6. The creation of an IG Steering Group would allow PSoS to specifically discuss data protection and information security training requirements. Once data protection training needs have been identified, the IG steering group can report back to the training committee. Please refer to recommendation a23 regarding the creation of an IG Steering Group.	**Management response:** **Accepted.** Information management training will constitute a standing item for the Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
b7. PSoS should implement this process as soon as is practicable and ensure that relevant staff across PSoS are made aware of the process.	**Management response:** **Partially accepted.** The Information Governance Steering Group will be responsible for ensuring a coherent programme of data protection training and awareness is in place. The training identification process will be a supplementary means by which training needs can be identified and		

	processed. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
b8. The responsibilities of subject matter experts and of IMT staff should be clarified to avoid the duplication of effort in the delivery of data protection training.	**Management response:** **Partially accepted.** The deployment of different officers and staff to undertake induction training, post-specific training and in-service awareness is considered to be an effective approach to training during an officer or member of staff's service. Nevertheless the responsibilities will be documented and potential overlaps subject to resolution by the Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 August 2016.		
b9. A training plan should be put in place that details the training requirements for all specialist data protection roles and the timescales in which	**Management response:** **Rejected.** The role profile for each role already specifies the level of knowledge and skill required, and PSoS will use the performance assessment		

they should be delivered from the start of employment.	methods to plan training requirements for individual members of staff. **Owner:** Not applicable **Date for implementation:** Not applicable		
b10. Please refer to recommendation at **b1**.	**Management response:** Please refer to recommendation at b1.		
b12. Completion level statistics for data protection training should be reported to the IG Steering Group (please refer to recommendation at **a23**) and if necessary, escalated to the CGB. Relevant training and awareness KPIs and targets should also be created and monitored as appropriate.	**Management response: Partially accepted.** Information management training will constitute a standing item for the Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
b13. The annual appraisal process should be restarted within the IMT so there can be an accurate assessment of individual staff acquired skills and ongoing development needs in regards to	**Management response: Rejected.** IMT staff will be subject to any appraisal process agreed with staff side associations for implementation across the Service. In the meantime, current performance assessment methods will be used.		

data protection.	**Owner:** not applicable **Date for implementation:** not applicable		
b15. The Information Sharing SOP should be reviewed on an annual basis to ensure it remains up to date and in line with current practice. Please refer to recommendation at a6.	**Management response:** **Partially accepted.** The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
b22. This audit activity should be completed as soon as is practicable and any recommendations implemented to ensure consistency and compliance in the use of the 'Section 29' process across PSoS.	**Management response:** **Accepted.** This activity is already ongoing, as noted in the report. **Owner:** Head of Information Management **Date for implementation:** 31 December 2016		
b24. Data sharing should be added as a standard agenda item for the IG Steering group to discuss any risks or concerns relating to current data sharing projects. Any risks identified should	**Management response:** **Partially accepted.** Information sharing will constitute a standing item for the Information Governance Steering Group. Information Management will continue to gather information about information sharing project		

be reported to the CGB if necessary. Please refer to recommendation **a23** regarding the creation of an IG Steering Group.	risks and concerns through Organisational Development. **Owner:** Head of Information Management. **Date for implementation:** 31 March 2017		
b25. The requirement to conduct a PIA for all new projects, including projects involving data sharing, should be documented in a policy or SOP. The policy or SOP should set out a clear process for determining when a PIA should be conducted, who it will be authorised by, how it will be incorporated into the project plan and how compliance will be monitored. The policy or SOP should clearly identify the roles responsible for completing PIAs.	**Management response:** **Partially accepted.** The requirement to conduct a PIA in certain circumstances will be set out in an appropriate PSoS SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c1. PSoS should introduce an Information Risk Strategy to set out how the organisation	**Management response:** **Partially accepted.** The manner in which PSoS manages information risk will be articulated in the		

will manage information risk specifically.	Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c7. Risks can be discussed at a lower level at the IG Steering Group (recommendation at **a23**) to consider the risks that require escalating to the CGB. The IG Steering Group should report on the information risk strategy recommended at **c1** and provide oversight of the information risk register recommended at **c4**.	**Management response:** **Accepted.** Information risk will constitute a standing item for the Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c10. In order to obtain adequate oversight and assurance, it would be good practice for the SIRO to not carry out separate roles, such as IAO, which may overlap with his SIRO responsibilities.	**Management response:** **Partially accepted.** The information governance framework already in place separates the roles of SIRO and IAO. The policy will be reviewed on appointment of a corporate director. **Owner:** Head of Information Management		

	Date for implementation: 31 March 2017		
c11. IAOs should receive training on a regular basis to ensure that they are aware of their roles and responsibilities. PSoS should provide training to new and existing IAOs as soon as practicable. PSoS should ensure that these responsibilities are also formally documented in job descriptions.	**Management response: Partially accepted.** Information governance roles and relationships will be articulated in an Information Governance SOP, rather than in job descriptions. Training will be provided to IAOs on approval of the Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c12. Operational Business Owners responsible for carrying out the operational aspects of the IAO role should be appointed as Information Asset Administrators (IAA). Formally document the roles of IAAs and IAOs to ensure that all information assets are being appropriately managed.	**Management response: Accepted.** Information governance roles and relationships will be articulated in an Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		

c13. PSoS should introduce a forum for IAOs to regularly meet with the SIRO and discuss issues relating to their role. Alternatively, IAOs can discuss relevant issues or concerns at the IG Steering Group (Please refer to recommendation at a23).	**Management response: Rejected.** PSoS considers that the Force Governance Board, the proposed Information Governance Steering Group and the establishment of formal reporting to the SIRO provide sufficient engagement opportunities to raise information governance issues. **Owner:** Not applicable **Date for implementation:** Not applicable		
c14 a) PSoS should introduce a comprehensive IAR containing all information assets including paper records. This should also identify IAOs for each asset and document the outcomes of periodic risk assessments of assets to ensure that the data held by each information system is controlled and kept	**Management response: Accepted.** The creation and maintenance of a detailed information asset register will be the responsibility of the Records Manager. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		

securely. **b)** PSoS should assign overall responsibility for maintaining the new IAR to an appropriate staff member and ensure that all policies and procedures that mention the IAR, such as the IT Systems Development SOP, are updated accordingly.			
c15. PSoS should introduce formal IAO reporting to the SIRO on a regular basis, for example, through the suggested IAO forum or through the IG Steering Group. This would ensure that all information assets are regularly risk assessed, and that the SIRO has appropriate oversight of how these risks are being managed.	**Management response: Partially accepted.** Information governance roles and relationships, including formal reporting relationships, will be articulated in an Information Governance SOP. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c16. Please refer to recommendation at	**Management response: Partially accepted.** Please		

b25 regarding the requirement to undertake PIAs.	refer to recommendation at b25. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c17. PSoS should consider basing any future PIA template on the PIA that was used for the 'Stop and Search' Project in 2013. As a minimum, PIAs should include a consultation process with the IMT and detail the results of the PIA including the proposed information flows, compliance risks and mitigating risks. You may wish to refer to our PIA Code of Practice for further guidance.	**Management response:** **Partially accepted.** The methodology for conducting a PIA will be set out in an appropriate PSoS SOP. Completed PIAs will be used by the IA team as exemplars. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c20. PSoS should ensure that risks identified via PIAs, as well as those identified through incident analysis and risk assessments of information assets,	**Management response:** **Partially accepted.** The manner in which PSoS manages information risk will be articulated in the Information Governance SOP. **Owner:** Head of Information		

feed into the organisation's risk management structures and are escalated appropriately. The PIA SOP recommended above should stipulate that this happens.	Management **Date for implementation:** 31 March 2017		
c21. Ensure the Information Security Policy and corresponding SOP are updated and reviewed annually. Please refer to recommendation at a6.	**Management response: Partially accepted.** The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
C22. Ensure all policies and SOPs are updated and reviewed annually. Please refer to recommendation at **a6**.	**Management response: Partially accepted.** The review period for all information management policies and SOPs will be re-considered in conjunction with Policy Support. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c23. PSoS should introduce a standalone	**Management response: Rejected.** PSoS consider it		

information security risk management policy to document how the organisation deals with information security risks.	is important to manage information security risk alongside other risks facing the Service to ensure a consistent approach to the assessment, mitigation, reporting and scrutiny of risk. The existing suite of SOPs for information security is considered sufficient. **Owner:** Not applicable **Date for implementation:** Not applicable		
c31. Review and update the ICT Systems Development SOP. Please refer to recommendation at a6. Risk assessments should be reviewed on a regular basis to reassess the level of risk. PSoS should ensure that implemented controls still appropriately address identified risks.	**Management response:** **Rejected.** Regular review of risk controls is already an established element in the PSoS approach to risk management. **Owner:** Not applicable **Date for implementation:** Not applicable		
c33. Please refer to the recommendation at a23 regarding the creation of an IG	**Management response:** **Accepted.** Information security will constitute a standing item for the		

Steering Group. Information security should be included as a standard agenda item and issues escalated to the CGB, where necessary.	Information Governance Steering Group. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		
c34. PSoS should formally document their information security work plan in order to monitor progress with projects and compliance deadlines.	**Management response:** **Partially accepted.** A composite work plan for the IA team will enable progress with projects to be monitored. **Owner:** Head of Information Management **Date for implementation:** 31 March 2017		

I can confirm that this management response is a true representation of the current situation regarding progress made against our Action Plan outlined in the ICO Data Protection Audit Report dated 9 September 2016.

Signature……

Position……

Organisation……