SCOTTISH POLICE AUTHORITY

Agenda Item 3d

Meeting	**Audit, Risk and Assurance Committee**
Date	**16 July 2020**
Location	**Video- conference**
Title of Paper	**Data Protection and Retention Internal Audit Report**
Presented By	**Gary Devlin, Partner, Scott-Moncrieff**
Recommendation to Members	**Members are requested to discuss the report.**
Appendix Attached	**Data Protection and Retention Internal Audit Report**

PURPOSE

This paper presents our final report on the review of Data Protection and Retention.

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

The paper is submitted for discussion.

1. BACKGROUND

1.1 The General Data Protection Regulations came into force in May 2018. This replaced the Data Protection Act 1998 and created a number of new requirements for organisations processing personal data. Part 3 of the Data Protection Act 2018 (DPA 2018), implemented the EU Law Enforcement Directive (Directive 2016/680) and sets out the obligations of law enforcement agencies which are separate from the GDPR regime.

1.2 It is essential for public trust that the Scottish Police Authority and Police Scotland implement formal policies and procedures to achieve compliance with legislative requirements. In addition, both organisations need to provide appropriate training to staff to support them in developing operational practices which are compliant with legislative requirements.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Our review of data protection and retention within SPA has identified several areas where there was a need to improve the control environment.

2.2 The most significant of these relates to the need for incidents to be notified to the Data Protection Officer (DPO) in accordance with policy so that they can be investigated and reported, if necessary, to the Information Commissioner’s Office (ICO). An incident in late January 2020 was not notified to the DPO by staff in Forensic Services and it was only identified through the vigilance of the DPO monitoring email filters. The incident was being investigated within FS but without the involvement of the DPO. This practice, if sustained, will increase the risk of significant financial penalty and negative publicity if data breaches are not managed appropriately.

2.3 In addition, we noted that there are no formal governance structures within SPA to support oversight and scrutinise data protection activity. For example, there is no management reporting on incidents that have occurred, the number of subject access requests received etc. We recognise that there has been challenges in continuity of leadership and reporting on Information Management due to the absence of a member of SPA senior management. The Director of Communications and Relationships assumed the role as Senior Information Risk Officer (SIRO) in

February 2020. He has identified that there is a need for improved communications, working arrangements and reporting and has commenced work to address this.

2.4 Our review has indicated that, in general, Police Scotland has controls consistent with leading practice in several areas. These include having a centralised system for the recording and tracking of data privacy impact assessments, data subject access requests and data security incidents. Our testing of a sample of data subject access requests identified that they were recorded appropriately and responded to in line with the requirements of the General Data Protection Regulations.

2.5 We have identified several areas where controls could be improved. The most significant of these relates to the completion of mandatory online training. In mid-February 2020, 65% of staff had completed the training. Whilst completion rates are being monitored and reported to senior management, additional measures such as restriction of network and internet access should be considered by management.

2.6 Police Scotland management is planning to develop a more strategic approach to data protection and retention. Much of the effort to date has been tactical and operational. Management should ensure that issues contained within this report, such as approaches to compliance, records retention and training, are factored into strategic objectives.

3. FINANCIAL IMPLICATIONS

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

4. PERSONNEL IMPLICATIONS

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

5. LEGAL IMPLICATIONS

5.1 The Internal Audit Report considers the extent of compliance within SPA and Police Scotland with applicable law in the area of Data Protection. Committee members should consider this section when considering the overall implications of our findings.

6. REPUTATIONAL IMPLICATIONS

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

7. SOCIAL IMPLICATIONS

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

8. COMMUNITY IMPACT

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

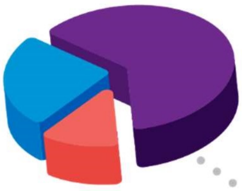
9. EQUALITIES IMPLICATIONS

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

10. ENVIRONMENT IMPLICATIONS

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

RECOMMENDATIONS
Members are requested to discuss the report.



Scottish Police Authority

Internal Audit Report 2020/21

Data protection and retention

June 2020

Scottish Police Authority

Internal Audit Report 2019/20

Data protection and retention

Audit Sponsor	***Key Contacts***	***Audit team***
ACC Alan Speirs, Police Scotland *Lynn Brown, Interim Chief Executive, Scottish Police Authority*	*Alice Stewart, Information Manager (Assurance), Police Scotland* *Joe Bartolleti, Records Manager, Police Scotland* *Lindsey Davie, Head of Information Management, Scottish Police Authority*	*Fraser Nicol, IT Audit Partner* *Paul Kelly, IT Audit Director* *Rachel Wilson, Senior IT Auditor* *Lara Boyaci, IT Auditor*

Introduction

Background

The General Data Protection Regulations came into force in May 2018. This replaced the Data Protection Act 1998 and created a number of new requirements for organisations processing personal data. Part 3 of the Data Protection Act 2018 (DPA 2018), implemented the EU Law Enforcement Directive (Directive 2016/680) and sets out the obligations of law enforcement agencies which are separate from the GDPR regime.

It is essential for public trust that the Scottish Police Authority and Police Scotland implement formal policies and procedures to achieve compliance with legislative requirements. In addition, both organisations need to provide appropriate training to staff to support them in developing operational practices which are compliant with legislative requirements.

Scope

The review considered the adequacy of processes within Police Scotland and SPA (both SPA Corporate and SPA Forensic Services) to achieve compliance with DPA 2018 and policies in relation to the storage and retention of personal data.

As Police Scotland and the Scottish Police Authority have separate processes and controls for data protection and retention, we have produced separate conclusions, key findings and management action plans for each organisation.

Acknowledgements

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

SPA – Executive Summary

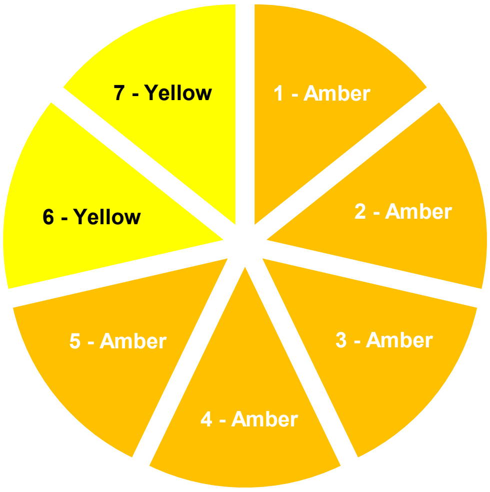
Conclusion

Our review of data protection and retention within SPA has identified several areas where there was a need to improve the control environment.

The most significant of these relates to the need for incidents to be notified to the Data Protection Officer (DPO) in accordance with policy so that they can be investigated and reported, if necessary, to the Information Commissioner's Office (ICO). An incident in late January 2020 was not notified to the DPO by staff in Forensic Services and it was only identified through the vigilance of the DPO monitoring email filters. The incident was being investigated within FS but without the involvement of the DPO. This practice, if sustained, will increase the risk of significant financial penalty and negative publicity if data breaches are not managed appropriately.

In addition, we noted that there are no formal governance structures within SPA to support oversight and scrutinise data protection activity. For example, there is no management reporting on incidents that have occurred, the number of subject access requests received etc. We recognise that there has been challenges in continuity of leadership and reporting on Information Management due to the absence of a member of SPA senior management. The Director of Communications and Relationships assumed the role as Senior Information Risk Officer (SIRO) in February 2020. He has identified that there is a need for improved communications, working arrangements and reporting and has commenced work to address this.

Control assessment



🟧 1. There are adequate policies and procedures in place to support staff in complying with the requirements of data protection legislation.

🟧 2. There are adequate policies and procedures for the identification, management and reporting of personal data breaches, including notification to the Information Commissioner's Office.

🟧 3. There are effective processes which ensure that Data Privacy Impact Assessments are performed whenever there is a new or revised activity that involves the processing of personal data.

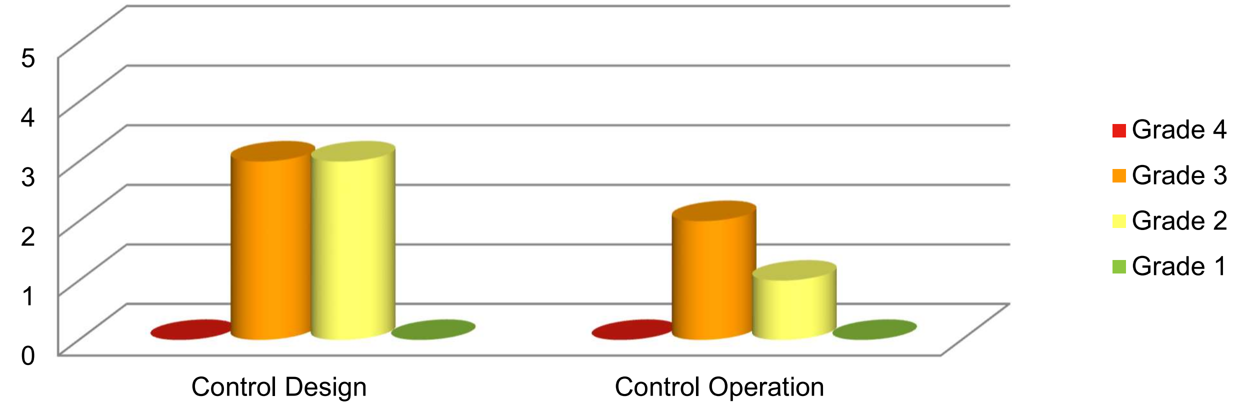
🟧 4. There are formal processes in place to monitor compliance with data protection legislation and the retention of personal data.

🟧 5. There are formal and effective processes for the management of data subject access requests as well as regular reporting to management on response performance.

🟨 6. There is adequate training and awareness provided to staff on data protection leading practices.

🟨 7. There are formal policies and procedures for ensuring that personal data is stored and retained in line with data protection legislation.

Improvement actions by type and priority



9 improvement actions have been identified from this review, 3 of which relate to compliance with existing procedures and 6 of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Good practice

We have gained assurance that SPA's procedures reflect good practice in a number of areas:

- Policies and procedures in place cover relevant areas of Data Protection, including guidance and template forms for handling Subject Access Requests, Data Protection Impact Assessments and Data Breaches.

- Mandatory training and awareness raising materials have been rolled out to both SPA and Forensic Service's (FS) staff.

Areas for improvement

We have identified a number of areas for improvement which, if addressed, would strengthen SPA control framework. These include:

- Reminding staff and management of the importance of reporting data security incidents to the Data Protection Officer within 24 hours and adhering to the data security incident management policy.

- Formalisation and documentation of the policy and procedure approval process.

- Reporting of data protection aspects such as data breaches and subject access requests to senior management and the SPA Audit Risk and Assurance Committee (ARAC) on a regular basis.

- Monitoring of compliance with policies and procedures, particularly where data protection regulations have stipulated timescales. For example, the requirement for high risk data breaches to be reported to the ICO within 72 hours or subject access requests to be responded to within one month.

These are further discussed in the Management Action Plan below.

Acknowledgements

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

SPA - Management Action Plan

Control Objective 1: There are adequate policies and procedures in place to support staff in complying with the requirements of data protection legislation.

Yellow

1.1 Review and update of policies and procedures

All policies and procedures state that they will be reviewed annually by the document owner however a number of policies and procedures have not been updated since May 2018: Information Security Standard Operating Procedure (SOP), Data Protection Policy, Data Protection Impact Assessment (DPIA) SOP and Subject Access Request (SAR) SOP.

Risk

There is a risk that policies and procedures do not reflect current practices due to failure to review and update annually, as stated within policy / procedure documents. This could result in outdated practices being followed by staff and increase the risk of non-compliance with regulatory obligations.

Recommendation

We recommend that policies and procedures are reviewed and updated annually by the document owner, in line with the Monitoring and Review controls outlined in each policy / procedure document.

When the review take place, the "Document Review" section of the policy / procedure should be updated for audit trail purposes.

We also recommend that a management or governance group within SPA has responsibility for oversight of policy updates.

Management Action

Grade 2 (Operation)

Management accept this recommendation.

The documents highlighted were reviewed and brought up to date in April 2020.

SPA Organisational Development (OD), currently ongoing, will include resources that have responsibility for matters including oversight of policy/procedures. A structure and process for review, management and approval of policy/procedures will be implemented on completion of the OD work and staff in posts

Action owner:	**Due Date:**
Head of IM (Annual review of policy/procedure)	Ongoing
Interim CE (OD implementation and oversight of policy/process)	Q4 20/21

1.2 Policy and procedure approval process

We were informed that currently, policies and procedures are issued to the Senior Information Risk Officer (SIRO) for approval. However, we identified that there is no formally documented process for the approval of policies and procedures.

Risk

There is a risk that policies and procedures are not subject to appropriate management approval. This could result in policies not fully reflecting the requirements and culture of the organisation and create uncertainty for staff and any third parties.

Recommendation

We recommend that the approval process for the creation or changes to policies and procedures is formally documented and shared with staff. The approval process should include a requirement for policies and procedures to have sign-off from SPA senior management.

Grade 2 (Design)

Management Action

Management accept this recommendation.

Refer to management response to 1.1

Action owner: Interim CE

Due date: Q4 2020/21

Control Objective 2: There are adequate policies and procedures for the identification, management and reporting of personal data breaches, including notification to the Information Commissioner's Office.

Amber

2.1 Compliance with Data Incident Management Policy

We identified an instance of non-compliance with the Data Incident Management Policy by Forensic Services. When incidents occur, they need to be notified to the DPO immediately to then allow a decision to be made on whether they need to be reported to the ICO within the 72-hour timeframe set out in DPA2018.

The incident, which occurred within Forensic Service, was not reported to the DPO (SPA Head of Information Management) within the required 24-hour timeframe. This only became known by the DPO through her own vigilance in monitoring email filters (an email which included security incident in the subject line was the trigger for this). In addition, we noted that it took several days and reminders for the contact in Forensic Services to provide any information to the DPO.

The incident, a package that was delivered to the wrong secure location, occurred on 29 January 2020 and was escalated to Forensic Services senior management on 31January 2020 following initial internal investigation. The item was recovered from the secure location on 3 February 2020. At that point, the investigation was stood down. The DPO became aware of the incident from review of email filters on 6 February 2020 and requested the incident report. On 10 February 2020, the DPO had to follow-up her email of 6 February 2020 for the incident report. The incident report was submitted by Forensic Services to the DPO on 10 February 2020.

We also identified from the reviewing the completed incident form that the reasoning behind the risk rating is unclear from both the Incident Log and the completed form.

There are no dedicated Information Management personnel within Forensic Services. The two members of the SPA Information Management team are based in Pacific Quay and have limited access to Forensic Services systems and data.

Risk

There is a risk that, if incidents are not reported in line with Data Incident Management Policy, data breaches will not be properly investigated and risk assessed to allow a determination to be made by the DPO on whether there is a need to report the incident to the ICO within 72 hours of the incident being identified. This could result in a significant financial penalties and negative publicity.

Recommendation

We recommend that senior SPA management emphasise the importance of complying with data protection and incident reporting procedures. This should be done in a manner which supports openness and transparency in reporting incidents. These messages should be reiterated periodically to support awareness of process and to build a positive data protection and incident reporting culture.

Consideration should be given to having members of the Information Management team based within Forensic Services teams on a regular basis e.g. 1-2 days per week. This should support better engagement between the Information Management team and Forensic Services staff.

We recommend that the incident log documents the rationale used in in determining the risk rating of incidents. Where incidents have not been reported to the ICO, the log should document the reasons as to why the incident did not need to be reported.

Grade 3 (Operation)

Management Action

Management accept this recommendation.

The Director of Forensic Services will re-iterate to staff via email the importance of reporting security incidents and shall ensure this message is re-enforced quarterly via quality leads.

Information Management will provide the Director of Forensic Services with reports where the policy is not complied with.

Members of the Information Management Team had started spending a minimum of one day a week within Forensic Services prior to ‘lockdown’. Consideration of Information Management resourcing requirements to support FS are being reviewed as part of the SPA OD work currently ongoing.

The ICO’s flowchart for decision making is used when deciding whether or not a security incident is reportable. The results will be formally recorded in future within each incident folder.

Action owner:	**Due date:**
Director of FS	Q2 2020/21
Interim CE (SPA Org Development)	Q4 2020/21
Head of IM (Reporting and managing recommendations)	Ongoing

2.2 Reporting of security incidents

We were informed that SPA security incidents are reported to the National Police Chiefs' Council on a quarterly basis. In addition, the Data Incident Management SOP (Standard Operating Procedure) states that a summary of security breaches will be reported to the Senior Management Group. However, we identified that there is no formal reporting of security incidents to SPA senior management, the Board or any of its committees.

We recognise that there have been challenges in continuity of line management and reporting for the Information Management team in the past 12-18 months due to the absence of a member of senior SPA management. The Director of Communications and Relationships assumed the role of SIRO in February 2020 and attended a formal training course prior to this. The issues around reporting have been identified by the SIRO and discussions have been held to address reporting issues as well as other issues identified in this report.

Risk

There is a risk that senior management and Board members will not be sufficiently aware of the adequacy of the data security environment and the frequency of incidents due to a lack of reporting. This could result in failure to ensure that actions are taken to address issues that contributed to security incidents, thereby increasing the likelihood of incidents recurring. This could result in non-compliance with legislation with the SPA potentially incurring significant financial penalty and reputational damage.

Recommendation

We recommend that the SPA Information Management team produces regular (e.g. quarterly) reports on security incidents to senior management and the SPA Audit Risk and Assurance Committee (ARAC). As a minimum, the report should include:

- The number of incidents which have occurred by type and risk rating.
- The number of incidents reported to the Information Commissioners Officer (ICO)
- A description of the incident for high risk-rated incidents
- Mitigating actions which have been taken following the incident
- The time taken between the incident occurring and the incident being reported to the Data Protection Officer (DPO).

We also recommend that there is regular monitoring of mitigating actions by senior management to confirm that they are being addressed.

Grade 3 (Design)

Management Action

Management accept this recommendation.

Information Management will prepare reports highlighting the information specified for the Chief Executive and Director of Forensic Services quarterly.

Reports will be submitted to the Audit Risk and Assurance Committee 6 monthly.

The FS Information Asset Owners shall monitor the effectiveness of mitigating actions and report quarterly to the SIRO/Chief Executive/Director of FS.

Action owner: Head of Information Management **Due date:** Q3 2020

Control Objective 3: There are effective processes which ensure that Data Privacy Impact Assessments are performed whenever there is a new or revised activity that involves the processing of personal data.

Amber

3.1 Tracking of data protection impact assessments

Our audit work identified that there is no tracker in place for Data Protection Impact Assessments (DPIAs). We understand from our discussions that there has been a low number of DPIAs performed with SPA.

We sought assurance on how SPA could be assured that DPIAs are performed for all new or revised activity that had potential impact on processing of personal data. It was stated that the Police Scotland ICT Team acts as gatekeepers and will not allow any new technology to go live without a completed DPIA. However, there is no assurance over non-ICT changes.

Risk

There is a risk that, if the Information Management team is not routinely engaged as part of project and change activity, management will have limited assurance that DPIAs are being completed where required. This could result in failure to complete a DPIA and mitigating controls not being implemented to protect personal data. This could increase the risk of non-compliance with legislation as well as significant financial penalties and reputation damage.

Recommendation

We recommend that a log is created and maintained by the Information Management team to record and track Data Protection Impact Assessments. The log should record instances where advice has been sought, instances where an assessment is currently being carried out and the status of the assessment.

We also recommend that the Information Management team is engaged by all areas of SPA as part of projects and change activities that could impact on the processing of personal data. The level of involvement in the process should be informed by any risks identified from the completion of a DPIA.

Management Action

Grade 3 (Design)

Management accept this recommendation.

An email will be sent by IM to staff reminding them of the need for DPIA's and early engagement with Information Management. A log will be created and maintained by Information Management to ensure all relevant information is captured.

Consideration as to how IM can become more aware of ongoing business activities in Forensic Services will be undertaken (such as involvement in IT meetings).

An early engagement process has been agreed with procurement to identify any relevant processing activities.

Action owner: Head of IM/Director FS **Due date:** Q3 2020

Control Objective 4: There are formal processes in place to monitor compliance with data protection legislation and the retention of personal data.

Amber

4.1 Monitoring of compliance with policies and procedures

A gap has been identified by the Information Management team in monitoring compliance with data protection procedures.

An area of concern they identified is compliance with the Retention Schedule in relation to electronic data. To allow the team to perform compliance reviews they identified that additional resources were needed. We noted that the team is currently going through a restructure and the DPO has reiterated the need for additional resources.

In the interim, we confirmed that there was some ad-hoc compliance monitoring through occasional reviewing of email filters.

Risk

There is a risk that, without formal compliance monitoring activities, management will not be able to confirm whether operational practices and processes are in compliance with policy requirements. This could result in failure to comply with regulatory requirements and potentially significant negative financial and reputation impact.

Recommendation

We recommend that, if the additional role is approved, management establishes and implements formal, risk-based compliance monitoring of data protection and retention activities.

A compliance plan/schedule should be produced and approved by management which sets out the planned compliance activities to be undertaken. This should include a timetable for all activities. When compliance activity is completed, the results of this should be presented to management along with any remedial actions that need to be addressed. Management should also consider how they can implement compliance reviews at line manager level within SPA to allow assurance to be gained that operational processes and practices are consistent with policy and procedures. This could include spot checks by line managers of compliance with clear desk policy.

If the additional role is not approved, management should evaluate how assurance can be gained using existing resources that high-risk areas of the SPA are in compliance with data protection and retention processes and procedures.

Grade 3 (Operation)

Management Action

Management accept this recommendation.

SPA Organisational Development (OD), currently ongoing, will include consideration of resource requirements to discharge all requirements in respect to Information Management

Following the completion of the OD work, if there are insufficient resources management will consider alternative arrangements to address the recommendation

Action owner: Interim CEO **Due date:** Q4 2020

Control Objective 5: There are formal and effective processes for the management for the management of data subject access requests as well as regular reporting to management on response performance.

Amber

5.1 Reporting of Data Subject Access Requests

We were informed that Data Subject Access Requests (SARs) are looked at by Information Management team on a weekly basis. However, we identified that there is no formal reporting of SARs to SMT or SPA ARAC.

We also identified that 7 out of the 11 requests received this financial year had not been responded to within the due date. We recognise that the seven requests formed part of a 'group' request, where seven individuals submitted the same questions. It was stated that the delay in responding was that the data being requested related to legacy data that pre-dated the creation of the SPA.

Risk

There is a risk that Senior Management are unaware of the completion rates in responding to SARs within the stipulated timescale of one month due to a lack of reporting. This could result in failure to identify resource requirements and operational requirements to ensure SARs are responded to within this timescale. Therefore, leading to further non-compliance and potentially fines.

Recommendation

We recommend that the Information Management Team regularly (at least quarterly) report against SARs to Senior Management and the SPA ARAC. The report should include the following:

1. The number of SARs received

2. The percentage of SARs responded to by the due date

3. Mitigating actions and / or lessons learned to improve the number of SARs responded to within regulatory timeframes.

Management Action

Grade 3 (Design)

Management accept this recommendation.

Information Management will provide quarterly reports to the SPA SIRO/Chief Executive in respect of subject access requests. Where there are any issues/delays identified reports will be prepared for the Audit, Risk and Assurance Committee.

Action owner: Head of Information Management **Due date:** Q3 2020

Control Objective 6: There is adequate training and awareness provided to staff on data protection leading practices.

Yellow

6.1 Monitoring of training completion rates

We were informed that data protection training is carried out using the Police Scotland Moodle training platform and Police Scotland can provide training completion rates for SPA Corporate and FS to the SPA Head of Information Management.

We also noted that there is no formal monitoring and reporting of training completion rates by SPA staff. At the time of our audit work, the latest information held was from 14 November 2018.

Risk

There is a risk that staff do not complete training and are unaware of their responsibilities due to training completion rates not being tracked. This could result in failure for staff to comply with regulatory requirements and therefore incompliance with the DPA 2018.

Recommendation

We recommend that the Information Management team requests and receives online training completion rates from Police Scotland on a regular basis e.g. monthly or quarterly.

These reports should be reviewed to identify any staff who have not yet completed the training. Those staff who have not completed the training should be reminded to do so. If staff persist in not completing the training, the issue should be escalated to their line manager and then to senior management, if necessary.

Management Action

Grade 2 (Design)

Management accept this recommendation.

SPA will be undertaking a review of training on Q4 2020 to ascertain the best way forward in terms of service provision. Any new solution will have full reporting capability and IM staff will work with HR staff to develop a mechanism for communication any issues to managers.

Where training issues are escalated to managers and training is still not completed the data will form part of the IM quarterly report on security issues to the CE and Director Forensic Services.

Action owner: Head of Information Management **Due date:** Q1 2021

Control Objective 7: There are formal policies and procedures for ensuring that personal data is stored and retained in line with data protection legislation.

Yellow

7.1 Clarity of decisions taken to inform retention periods within the retention schedule

A retention schedule is in place and is split up by functional area. The schedule includes a description of the process, retention action (period), examples of records and notes such as best practice or statutory obligations.

However, we found that instances where "archive" had been noted as the retention action and did not state how long records should remain in easily accessible systems and onsite physical storage before being archived. For example, "Register of Surgeons" under the process of “managing police casualty surgeons’ lists” states the action as archive only but no time periods are stated.

We also identified instances where the examples of records and notes sections are blank, and it is therefore unclear as to what has informed the retention period (e.g. legal / regulatory compliance or business purpose).

Risk

There is a risk that data is archived before it has fulfilled its processing requirements due to unclear timeframes documented within the schedule. This could negatively impact the availability of data for staff and cause operational inefficiencies.

Recommendation

We recommend that where "archive" has been recorded as the retention action, the schedule is updated to record the time period for which the document is required to be easily accessible for processing purposes.

We also recommend that the schedule notes the reasoning behind the documented retention action to allow individuals, particularly those who will have to review the Record Retention SOP in the future, to understand where requirements are to meet regulatory and legislative requirements, and where retention periods have been decided on business purposes.

Management Action

Grade 2 (Design)

Management accept this recommendation.

The document is owned by Police Scotland. The SPA Records Manager will engage with Police Scotland to make the necessary updates.

Action owner: Records Manager

Due date: Q4 2020

Police Scotland – Executive Summary

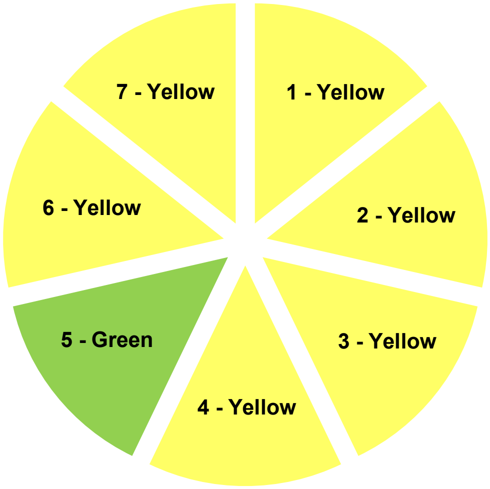
Conclusion

Our review has indicated that, in general, Police Scotland has controls consistent with leading practice in several areas. These include having a centralised system for the recording and tracking of data privacy impact assessments, data subject access requests and data security incidents. Our testing of a sample of data subject access requests identified that they were recorded appropriately and responded to in line with the requirements of the General Data Protection Regulations.

We have identified several areas where controls could be improved. The most significant of these relates to the completion of mandatory online training. In mid-February 2020, 65% of staff had completed the training. Whilst completion rates are being monitored and reported to senior management, additional measures such as restriction of network and internet access should be considered by management.

Police Scotland management is planning to develop a more strategic approach to data protection and retention. Much of the effort to date has been tactical and operational. Management should ensure that issues contained within this report, such as approaches to compliance, records retention and training, are factored into strategic objectives.

Control assessment



🟨 1. There are adequate policies and procedures in place to support staff in complying with the requirements of data protection legislation.

🟨 2. There are adequate policies and procedures for the identification, management and reporting of personal data breaches, including notification to the Information Commissioner’s Office.

🟨 3. There are effective processes which ensure that Data Privacy Impact Assessments are performed whenever there is a new or revised activity that involves the processing of personal data.

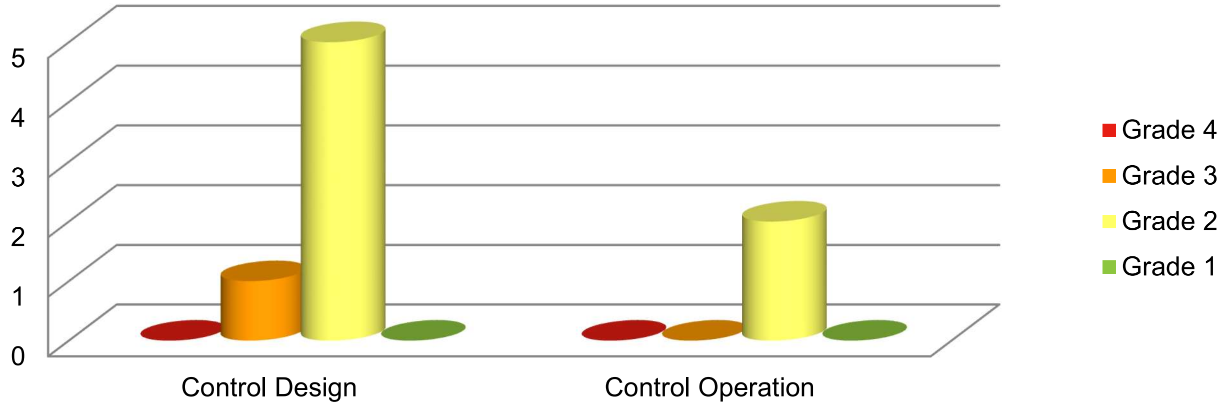
🟨 4. There are formal processes in place to monitor compliance with data protection legislation and the retention of personal data.

🟩 5. There are formal and effective processes for the management of data subject access requests as well as regular reporting to management on response performance.

🟨 6. There is adequate training and awareness provided to staff on data protection leading practices.

🟨 7. There are formal policies and procedures for ensuring that personal data is stored and retained in line with data protection legislation.

Improvement actions by type and priority



8 improvement actions have been identified from this review, 2 of which relate to compliance with existing procedures and 6 of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Good practice

We have gained assurance that Police Scotland's procedures reflect good practice in a number of areas, including:

- Online training is available to all staff through the Moodle training platform. The training is engaging and controls are in place to ensure staff cannot skip through content.
- The SharePoint system is used effectively for logging and tracking the status of data breaches, subject access requests and data protection impact assessments.
- Our sample testing of data subject access requests identified that all had been recorded and were responded to within one calendar month.
- Various working groups have formed to make decisions about, and action, the destruction of physical data in line with the retention schedule.

Areas for improvement

We have identified a number of areas for improvement which, if addressed, would strengthen Police Scotland's control framework. These include:

- Improving the completion rates of the Moodle training across all business areas. At the time of our review, only 65.3% of staff had completed training.
- Increasing the types of compliance monitoring activities undertaken to ensure that staff are following policies and procedures e.g. spot checks carried out by line managers
- Continuing to monitor the improve the retention of records in line with the retention schedule, particularly focusing on the retention of electronic data following the physical data weeding project.

These are further discussed in the Management Action Plan below.

Acknowledgements

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

Police Scotland - Management Action Plan

Control Objective 1: There are adequate policies and procedures in place to support staff in complying with the requirements of data protection legislation.

Yellow

1.1 Review and update of policies and procedures

Although policies and procedures state that they will be reviewed by the document owner annually, the majority of policies and procedures have not been reviewed since May 2018. For example, the data protection policy is dated 25 May 2018. We noted other policies which have not been updated for over six years e.g. the Information Security and Records Management policies were last updated on 7 February 2014.

It has also been identified by Police Scotland management that there is a need to reduce the volumes of SOPs and consolidate some of them to make them easier to manage and maintain as well as reducing the risk of duplication.

We were informed that new versions of the Record Retention SOP, Information Governance SOP and consolidated Security SOP are due to go to Policy Support team for mandatory consultation by 1 August 2020. The Information Management team is aware that other policies need to be reviewed and updated, however these three SOPs were identified as the high priority areas.

Risk

There is a risk that the policies and procedures in place no longer reflect current practices and legal requirements. This could result in staff practices not being consistent with legal and regulatory requirements, increasing the potential for financial penalty and negative publicity.

Recommendation

We recommend that policies and procedures are reviewed and updated at least annually. To ensure that reviews are completed, we recommend that the Information Management Team log and track policies and procedures currently in place, their last review date and the due date of the next review. The Information Governance Board should seek assurance on a regular basis that policies are being reviewed in line with their agreed frequency.

Grade 2 (Operation)

Management Action

Management accept this recommendation.

Information Management (IM) will support the established governance process for the Police Scotland Record Set.

IM will identify any updates to SOPs, guidance and forms required due to any known legislation, process, and structural changes and develop plans for these Casual Reviews.

We recognise that cyclical reviews are set as part of the Executive Approval process based on a subjective assessment of the corporate and operational risk of each document based on the principles set out in the Risk Management SOP.

IM will support the Responsible Person in the review and development of any IM SOPs /documents identified by Policy Support as the subject of review for 2020/21.

Action owner: Head of Information Management **Due date:** 1 January 2021

1.2 Communication of roles and responsibilities

The roles and responsibilities involved in data protection activities are not consistently set out within policy and procedure documentation.

The Data Protection SOP only contains information on the role of the Data Protection Officer and whilst the draft Information Governance SOP and some of the more detailed SOPs, such as the Information Security SOP, does cover roles and responsibilities, this is not consistently done across all SOPs. For example, the roles and responsibilities involved in managing, responding to, and reporting on Subject Access Requests is unclear.

Risk

There is a risk that staff are unaware of their responsibilities in relation to specific data protection activities due to a lack of clarity within policy and procedure documentation. This could result in staff not carrying out tasks which increases the risk of non-compliance with DPA2018.

Recommendation

We recommend that a review is undertaken of all approved and draft data protection-related SOPs to ensure that they clearly specify roles and responsibilities of all individuals who have specific or general data protection responsibilities.

Grade 2 (Design)

Management Action

Management accepts this recommendation.

Work is ongoing at the moment in relation to reviewing SOPs.

A review of clarity around roles and responsibilities will be included as part of any SOP Cyclical/Casual review process.

As part of this we will ensure that:

- Roles and responsibilities are clarified, reviewed and streamlined within SOPs.
- Re-design intranet mini site to contain guidance for DP including templates and contacts.

Action owner: Head of Information Management **Due date:** 1 January 2021

Control Objective 2: There are adequate policies and procedures for the identification, management and reporting of personal data breaches, including notification to the Information Commissioner's Office.

Yellow

2.1 Reporting of Security Incidents

Our review found that security Incidents are reported to the PS Audit and Risk Board on a quarterly basis. Reports break down the incidents that have occurred over the period by type and RAG (red, amber, green) rating. However, the report does not set out mitigating actions / lessons learned following the incident.

Risk

There is a risk that senior management will not have assurance that appropriate mitigations are in place to reduce the risk of incidents recurring. This could result in negative publicity for management if repeat incidents were to reoccur.

Recommendation

We recommend that the format of the Quarterly Security Incident Reports is updated to include relevant information on mitigating actions and process improvements which have been implemented in response to incidents that have occurred. This could also include details of changes recommended by the Information Management that departments or management have responsibility for implementing.

Grade 2 (Design)

Management Action

Management accept this recommendation.

An overview of mitigating actions/improvements will be reported, along with any exceptional individual instances.

We will provide information on remediation recommendations/mitigating actions where a high risk to individuals' rights has been identified and/or where there is a significant financial/legal/reputational risk to Police Scotland

We will revise the Security Incident Reporting template to include mitigation and process improvements (where identified).

Action owner: Head of Information Management **Due date:** 1 January 2021

Control Objective 3: There are effective processes which ensure that Data Privacy Impact Assessments are performed whenever there is a new or revised activity that involves the processing of personal data.

Yellow

3.1 Documentation of decisions to carry out full DPIAs

The DPIA form template does not currently require the risk level assigned to the project following the risk assessment to be included in the form. It is unclear, from reviewing the form alone, why a full DPIA was / was not required.

Risk

There is a risk that Police Scotland cannot adequately evidence the reasoning behind decisions to carry out, or not to carry out, a full DPIA. This could result in failure to comply with DPA2018 and potential financial penalties.

Recommendation

We recommend that the DPIA template form is updated to require a risk rating to be included, as well as the reasoning behind the risk rating, within the first part of the template.

Grade 2 (Design)

Management Action

Management accept this recommendation

We will amend the DPIA template to record rationale and reasoning behind the risk rating.

Action owner: Head of Information Management **Due date:** 1 January 2021

Control Objective 4: There are formal processes in place to monitor compliance with data protection legislation and the retention of personal data.

Yellow

4.1 Policy and procedure compliance monitoring

A Compliance Audit Schedule is in place. This is submitted annually to the Information Governance Board to identify high risk areas and define the audit programme for Information Assurance to deliver.

However, we noted that there are no compliance activities assigned to line managers/senior management to confirm that operational processes and procedures within their respective areas of responsibility are consistent with the requirements set out within policies and SOPs e.g. spot checks of compliance with clear desk policy etc.

We did note that the DPO has been absent for a prolonged period and Police Scotland intend to appoint an interim DPO in the near future.

Risk

There is a risk that compliance monitoring is seen as the responsibility of the Information Assurance team. This could result in a failure to identify and resolve local instances of failure to comply with policy and SOPs with the potential that issues could result in a breach of legislation and significant financial penalties.

Recommendation

We recommend that management develops additional compliance checks in addition to those to be performed by the Information Assurance team. This could include spot checks on areas such as clear desk policy, confirming that data sharing is performed in line with data sharing agreements. This could also include confirming that DPIAs, SARs, and data breaches logged on the SharePoint system have a completed form saved to the relevant file on the network and have been closed as appropriate. Other examples could include spot checks by the Portfolio Management Group to ensure that a DPIA has been completed for relevant projects and initiatives.

We also recommend that management considers appointing a deputy to the DPO or providing additional resiliency and capability to enable someone to deputise for the DPO in their absence. This will reduce the risk of over-reliance on a key individual.

The approach to both of these recommendations could be considered as part of a wider strategic approach to DPA2018 compliance.

Grade 2 (Design)

Management Action

Management accept this recommendation.

IM will continue to promote DP training and for Divisions drive Tier 1 and manage Tier 2 compliance.

We recognise the need for resilience around the DPO role and will develop options for consideration.

In order to achieve this, we will focus on the following actions:

- Introduce standard agenda item on compliance at both Data Governance Board and Professionalism & Assurance Strategy Group.
- Develop communication plan and guidance in relation to line manager responsibilities to conduct spot checks.
- Develop audit plan for Tier 2 compliance.
- Police Scotland management to consider options for providing additional resiliency to the DPO role.

Action owner: Head of Information Management **Due date:** 1 January 2021

Control Objective 5: There are formal and effective processes for the management for the management of data subject access requests as well as regular reporting to management on response performance.

Green

No significant control weaknesses identified.

Our audit testing of a sample of data subject access requests did not identify any control weaknesses. We found that a record is maintained of all subject access requests received, when they were received and when they were responded to. All subject access requests were responded to within the one calendar month requirement of the General Data Protection Regulations.

There is also reporting of performance on subject access requests to the Information Governance Board.

Control Objective 6: There is adequate training and awareness provided to staff on data protection leading practices.

Yellow

6.1 Training Completion Rates

We reviewed training content for each package (five in total) and found that training was created to be relevant for each role.

We also identified that training completion rates were low. Our review found that completion rates were 57.9% at 3 January 2020, increasing to 65.3% by 12 February 2020.

The Information Management team currently chase up individuals who have not completed training by issuing emails to senior members of each department listing those who have not completed training within expected timeframes. Completion rates are also reported monthly to the Force Executive.

Risk

There is a risk that staff are unaware of their responsibilities and lack understanding of relevant data protection regulations due to failure to complete training. This could result in failure to carry out work tasks in line with regulations with an increased risk of data breaches and resultant financial penalties as well as reputational damage.

Recommendation

We recommend that further action is taken to improve data protection training completion rates. We recommend that this is done by regularly reporting on training completion rates to a senior level forum which has the ability and authority to feed down to the relevant business areas the value that completing training has and the importance of doing so.

Management should also consider further options in cases where failure to complete training persists. For example, restricting access to high risk data or systems, removing access to the internet etc.

Grade 2
(Design)

Management Action

Management partially accept this recommendation.

Regular monitoring of compliance is conducted but we will consider options to improve governance and escalation processes for non-compliance. As of June 2020, the completion rate has increased to 75%.

Work is ongoing to implement additional controls to improve compliance rates. We will ensure regular updates are provided to Divisions on responsibilities for monitoring their own compliance and completion rates.

In relation to the second part of the recommendation, we will consider further options available and determine acceptable levels of tolerance for completion rates in consideration of individuals being absent or without IT access.

Action owner: Head of Information Management **Due date:** 1 April 2021

Control Objective 7: There are formal policies and procedures for ensuring that personal data is stored and retained in line with data protection legislation.

Yellow

7.1 Compliance with Retention Schedules

It has been identified by the organisation that there is still not 100% compliance with Retention Schedule set out within the Record Retention SOP. However, there are various ongoing activities in place to ensure that data held is in line with retention requirements. Examples include:

- Data Retention & Review Design Authority
- GDPR Structured / Unstructured Project
- Tender to amalgamate the disparate former storage and disposal facilities
- SCD (specialised crime division) Data Retention & Review Group
- Data Weeding & Destruction Working Group

The data weeding project has received funding that will allow it to continue until at least March 2021. It unclear how the organisation will continue to ensure that compliance with retention schedules is achieved and the monitoring of this.

Risk

There is a risk that data which should have been disposed of is still held by the organisation due to failure to comply with the Retention Schedule. This could result in failure to comply with data protection legislation and procedures leading to financial implications and reputational damage.

Recommendation

We recommend that the Records Manager continues to monitor compliance with the Retention Schedule. Areas which are of high risk should be prioritised and assigned budget, where possible, from the ongoing data weeding project.

We also recommend that management establishes formal processes and governance arrangements to monitor compliance with the Record Retention SOP following completion of projects. Consideration should be given to the resource requirements to support this centrally and at departmental level.

Grade 2 (Operation)

Management Action

Management accept this recommendation.

Work is already progressing in this area. Compliance will be driven and monitored by DRRDA.

The following actions will be undertaken:

- Review ToR of DRRDA to drive and monitor compliance. Extend remit of the forum to include hard copy, structured and unstructured data and widen membership.
- RM will continue monitor compliance and resource/funding to high risk areas.
- IM to document compliance governance and escalation processes for non-compliance with the Record Retention SOP.
- A risk road map will be produced to document activity alongside how and when these risks can reduce.

The timescales allow us to evidence progress alongside Record Management's application of central compliance.

Action owner: Head of Information Management **Due date:** 1 April 2021

7.2 There are formal policies and procedures for ensuring that personal data is stored and retained in line with data protection legislation.

A retention schedule is in place and is split up by functional area. The schedule includes a description the process, retention action (period), examples of records and notes such as best practice or statutory obligations.

However, we found that instances where "archive" had been noted as the retention action did not state how long records should remain in easily accessible systems and onsite physical storage before being archived. e.g. "Register of Surgeons" under the process of managing police casualty surgeons' lists states the action as archive only but no time periods are stated.

We also identified instances where the examples of records and notes sections are blank, and it is therefore unclear as to what has informed the retention period (e.g. legal / regulatory compliance or business purpose).

Risk

There is a risk that data is archived before it has fulfilled its processing requirements due to unclear timeframes documented within the schedule. This could negatively impact the availability of data for staff and therefore cause operational inefficiencies.

Recommendation

We recommend that where "archive" has been recorded as the retention action, the schedule records the time period for which the document is required to be easily accessible for processing purposes.

We also recommend that the schedule notes the reasoning behind the documented retention action to allow individuals, particularly those who will have to review the Record Retention SOP in the future, to understand where requirements are to meet regulatory and legislative requirements, and where retention periods have been decided on business purposes.

Management Action

Grade 2 (Design)

Management accept this recommendation.

Work is progressing in this area. The retention schedules will note specific reasoning for 'archive' actions and will be included in revised SOPs

Action owner: Head of Information Management **Due date:** 1 April 2021

Appendix A – Definitions

Control assessments

- R Fundamental absence or failure of key controls.
- A Control objective not achieved - controls are inadequate or ineffective.
- Y Control objective achieved - no major weaknesses but scope for improvement.
- G Control objective achieved - controls are adequate, effective and efficient.

Management action grades

4

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

3

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

2

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

1

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

Appendix B – SPA Action Summary

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
1.1	We recommend that policies and procedures are reviewed and updated annually by the document owner, in line with the Monitoring and Review controls outlined in each policy / procedure document. When the review take place, the "Document Review" section of the policy / procedure should be updated for audit trail purposes. We also recommend that a management or governance group within SPA has responsibility for oversight of policy updates.	Management accept this recommendation. The documents highlighted were reviewed and brought up to date in April 2020. SPA Organisational Development (OD), currently ongoing, will include resources that have responsibility for matters including oversight of policy/procedures. A structure and process for review, management and approval of policy/procedures will be implemented on completion of the OD work and staff in posts	2	Head of IM Interim CE	Ongoing Q4 20/21
1.2	We recommend that the approval process for the creation or changes to policies and procedures is formally documented and shared with staff. The approval process should include a requirement for policies and procedures to have sign-off from SPA senior management.	Management accept this recommendation. Refer to management response to 1.1	2	Interim CE	Q4 20/21
2.1	We recommend that senior SPA management emphasise the importance of complying with data protection and incident reporting procedures. This should be done in a	Management accept this recommendation. The Director of Forensic Services will re-iterate to staff via email the	3	Director of FS Interim CE Head of IM	Q2 20/21 Q4 20/21 Ongoing

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	manner which supports openness and transparency in reporting incidents. These messages should be reiterated periodically to support awareness of process and to build a positive data protection and incident reporting culture. Consideration should be given to having members of the Information Management team based within Forensic Services teams on a regular basis e.g. 1-2 days per week. This should support better engagement between the Information Management team and Forensic Services staff. We recommend that the incident log documents the rationale used in in determining the risk rating of incidents. Where incidents have not been reported to the ICO, the log should document the reasons as to why the incident did not need to be reported.	importance of reporting security incidents and shall ensure this message is re-enforced quarterly via quality leads. Information Management will provide the Director of Forensic Services with reports where the policy is not complied with. Members of the Information Management Team had started spending a minimum of one day a week within Forensic Services prior to 'lockdown'. Consideration of Information Management resourcing requirements to support FS are being reviewed as part of the SPA OD work currently ongoing. The ICO's flowchart for decision making is used when deciding whether or not a security incident is reportable. The results will be formally recorded in future within each incident folder.			
2.2	We recommend that the SPA Information Management team produces regular (e.g. quarterly) reports on security incidents to senior management and the SPA Audit Risk and Assurance Committee (ARAC). As a minimum, the report should include:	Management accept this recommendation. Information Management will prepare reports highlighting the information specified for the Chief Executive and Director of Forensic Services quarterly. Reports will be submitted to the Audit Risk and	3	Head of IM	Q3 2020

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	The number of incidents which have occurred by type and risk rating. The number of incidents reported to the Information Commissioners Officer (ICO) A description of the incident for high risk-rated incidents Mitigating actions which have been taken following the incident The time taken between the incident occurring and the incident being reported to the Data Protection Officer (DPO). We also recommend that there is regular monitoring of mitigating actions by senior management to confirm that they are being addressed.	Assurance Committee 6 monthly. The FS Information Asset Owners shall monitor the effectiveness of mitigating actions and report quarterly to the SIRO/Chief Executive/Director of FS.			
3.1	We recommend that a log is created and maintained by the Information Management team to record and track Data Protection Impact Assessments. The log should record instances where advice has been sought, instances where an assessment is currently being carried out and the status of the assessment. We also recommend that the Information Management team is engaged by all areas of SPA as part of projects and change activities that could impact on the	Management accept this recommendation. An email will be sent by IM to staff reminding them of the need for DPIA's and early engagement with Information Management. A log will be created and maintained by Information Management to ensure all relevant information is captured. Consideration as to how IM can become more aware of ongoing business activities in Forensic Services will be undertaken (such as involvement in IT meetings).	3	Head of IM Director of FS	Q3 2020

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	processing of personal data. The level of involvement in the process should be informed by any risks identified from the completion of a DPIA.	An early engagement process has been agreed with procurement to identify any relevant processing activities.			
4.1	We recommend that, if the additional role is approved, management establishes and implements formal, risk-based compliance monitoring of data protection and retention activities. A compliance plan/schedule should be produced and approved by management which sets out the planned compliance activities to be undertaken. This should include a timetable for all activities. When compliance activity is completed, the results of this should be presented to management along with any remedial actions that need to be addressed. Management should also consider how they can implement compliance reviews at line manager level within SPA to allow assurance to be gained that operational processes and practices are consistent with policy and procedures. This could include spot checks by line managers of compliance with clear desk policy. If the additional role is not approved, management	Management accept this recommendation. SPA Organisational Development (OD), currently ongoing, will include consideration of resource requirements to discharge all requirements in respect to Information Management Following the completion of the OD work, if there are insufficient resources management will consider alternative arrangements to address the recommendation	3	Interim CEO	Q4 2020

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	should evaluate how assurance can be gained using existing resources that high-risk areas of the SPA are in compliance with data protection and retention processes and procedures.				
5.1	We recommend that the Information Management Team regularly (at least quarterly) report against SARs to Senior Management and the SPA ARAC. The report should include the following: 1. The number of SARs received 2. The percentage of SARs responded to by the due date 3. Mitigating actions and / or lessons learned to improve the number of SARs responded to within regulatory timeframes.	Management accept this recommendation. Information Management will provide quarterly reports to the SPA SIRO/Chief Executive in respect of subject access requests. Where there are any issues/delays identified reports will be prepared for the Audit, Risk and Assurance Committee.	3	Head of IM	Q3 2020
6.1	We recommend that the Information Management team requests and receives online training completion rates from Police Scotland on a regular basis e.g. monthly or quarterly. These reports should be reviewed to identify any staff who have not yet completed the training. Those staff who have not completed the training should be reminded	Management accept this recommendation. SPA will be undertaking a review of training on Q4 2020 to ascertain the best way forward in terms of service provision. Any new solution will have full reporting capability and IM staff will work with HR staff to develop a mechanism for communication any issues to managers.	2	Head of IM	Q1 2021

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	to do so. If staff persist in not completing the training, the issue should be escalated to their line manager and then to senior management, if necessary.	Where training issues are escalated to managers and training is still not completed the data will form part of the IM quarterly report on security issues to the CE and Director Forensic Services.			
7.1	We recommend that where "archive" has been recorded as the retention action, the schedule is updated to record the time period for which the document is required to be easily accessible for processing purposes. We also recommend that the schedule notes the reasoning behind the documented retention action to allow individuals, particularly those who will have to review the Record Retention SOP in the future, to understand where requirements are to meet regulatory and legislative requirements, and where retention periods have been decided on business purposes.	Management accept this recommendation. The document is owned by Police Scotland. The SPA Records Manager will engage with Police Scotland to make the necessary updates.	2	Records Manager	Q4 2020

Appendix C – Police Scotland Action Summary

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
1.1	We recommend that policies and procedures are reviewed and updated at least annually. To ensure that reviews are completed, we recommend that the Information Management Team log and track policies and procedures currently in place, their last review date and the due date of the next review. The Information Governance Board should seek assurance on a regular basis that policies are being reviewed in line with their agreed frequency.	Management accept this recommendation. Information Management (IM) will support the established governance process for the Police Scotland Record Set. IM will identify any updates to SOPs, guidance and forms required due to any known legislation, process, and structural changes and develop plans for these Casual Reviews. We recognise that cyclical reviews are set as part of the Executive Approval process based on a subjective assessment of the corporate and operational risk of each document based on the principles set out in the Risk Management SOP. IM will support the Responsible Person in the review and development of any IM SOPs /documents identified by Policy Support as the subject of review for 2020/21.	2	Head of IM	Jan 2021
1.2	We recommend that a review is undertaken of all approved and draft data protection-related SOPs to	Management accepts this recommendation.	2	Head of IM	Jan 2021

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	ensure that they clearly specify roles and responsibilities of all individuals who have specific or general data protection responsibilities.	Work is ongoing at the moment in relation to reviewing SOPs. A review of clarity around roles and responsibilities will be included as part of any SOP Cyclical/Casual review process. As part of this we will ensure that: • Roles and responsibilities are clarified, reviewed and streamlined within SOPs. • Re-design intranet mini site to contain guidance for DP including templates and contacts.			
2.1	We recommend that the format of the Quarterly Security Incident Reports is updated to include relevant information on mitigating actions and process improvements which have been implemented in response to incidents that have occurred. This could also include details of changes recommended by the Information Management that departments or management have	Management accept this recommendation. An overview of mitigating actions/improvements will be reported, along with any exceptional individual instances. We will provide information on remediation recommendations/mitigating actions where a high risk to individuals' rights has been identified and/or where there is a significant financial/legal/reputational risk to Police Scotland We will revise the Security Incident Reporting template to include mitigation and process	2	Head of IM	Jan 2021

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	responsibility for implementing.	improvements (where identified).			
3.1	We recommend that the DPIA template form is updated to require a risk rating to be included, as well as the reasoning behind the risk rating, within the first part of the template.	Management accept this recommendation We will amend the DPIA template to record rationale and reasoning behind the risk rating.	2	Head of IM	Jan 2021
4.1	We recommend that management develops additional compliance checks in addition to those to be performed by the Information Assurance team. This could include spot checks on areas such as clear desk policy, confirming that data sharing is performed in line with data sharing agreements. This could also include confirming that DPIAs, SARs, and data breaches logged on the SharePoint system have a completed form saved to the relevant file on the network and have been closed as appropriate. Other examples could include spot checks	Management accept this recommendation. IM will continue to promote DP training and for Divisions drive Tier 1 and manage Tier 2 compliance. We recognise the need for resilience around the DPO role and will develop options for consideration. In order to achieve this, we will focus on the following actions: • Introduce standard agenda item on compliance at both Data Governance Board and Professionalism & Assurance Strategy Group. • Develop communication plan and guidance in relation to line manager responsibilities to conduct spot checks. • Develop audit plan for Tier 2 compliance. • Police Scotland management to consider	2	Head of IM	Jan 2021

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	by the Portfolio Management Group to ensure that a DPIA has been completed for relevant projects and initiatives. We also recommend that management considers appointing a deputy to the DPO or providing additional resiliency and capability to enable someone to deputise for the DPO in their absence. This will reduce the risk of over-reliance on a key individual. The approach to both of these recommendations could be considered as part of a wider strategic approach to DPA2018 compliance.	options for providing additional resiliency to the DPO role.			
6.1	We recommend that further action is taken to improve data protection training completion rates. We recommend that this is done by regularly reporting on training completion rates to a senior level forum which has the ability and authority to feed down to the relevant business areas the	Management partially accept this recommendation. Regular monitoring of compliance is conducted but we will consider options to improve governance and escalation processes for non-compliance. As of June 2020, the completion rate has increased to 75%. Work is ongoing to implement additional controls to improve compliance rates. We will	2	Head of IM	Apr 2021

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	value that completing training has and the importance of doing so. Management should also consider further options in cases where failure to complete training persists. For example, restricting access to high risk data or systems, removing access to the internet etc.	ensure regular updates are provided to Divisions on responsibilities for monitoring their own compliance and completion rates. In relation to the second part of the recommendation, we will consider further options available and determine acceptable levels of tolerance for completion rates in consideration of individuals being absent or without IT access.			
7.1	We recommend that the Records Manager continues to monitor compliance with the Retention Schedule. Areas which are of high risk should be prioritised and assigned budget, where possible, from the ongoing data weeding project. We also recommend that management establishes formal processes and governance arrangements to monitor compliance with the Record Retention SOP following completion of projects. Consideration should be given to the resource	Management accept this recommendation. Work is already progressing in this area. Compliance will be driven and monitored by DRRDA. The following actions will be undertaken: • Review ToR of DRRDA to drive and monitor compliance. Extend remit of the forum to include hard copy, structured and unstructured data and widen membership. • RM will continue monitor compliance and resource/funding to high risk areas. • IM to document compliance governance and escalation processes for non-compliance with the Record Retention SOP.	**2**	**Head of IM**	**Apr 2021**

Action No.	Recommendation	Management Response	Grade	Action Owner	Due Date
	requirements to support this centrally and at departmental level.	• A risk road map will be produced to document activity alongside how and when these risks can reduce. The timescales allow us to evidence progress alongside Record Management's application of central compliance.			
7.2	We recommend that where "archive" has been recorded as the retention action, the schedule records the time period for which the document is required to be easily accessible for processing purposes. We also recommend that the schedule notes the reasoning behind the documented retention action to allow individuals, particularly those who will have to review the Record Retention SOP in the future, to understand where requirements are to meet regulatory and legislative requirements, and where retention periods have been decided on business purposes.	Management accept this recommendation. Work is progressing in this area. The retention schedules will note specific reasoning for 'archive' actions and will be included in revised SOPs	2	Head of IM	Apr 2021