SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee Public Session**
Date	**22 January 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**SPA and Police Scotland Internal GDPR Additional Preparedness**
Item Number	**9.1**
Presented By	**Paul Kelly**
Recommendation to Members	**For Noting**
Appendix Attached	**No**

PURPOSE

This paper presents our final report on the review of GDPR (EU General Data Protection Regulation) readiness within Police Scotland and SPA (including Forensic Services).

The paper is presented in line with the Internal Audit contract with Scottish Police Authority.

The paper is submitted for consultation.

1. BACKGROUND

1.1 On 25 May 2018, the EU General Data Protection Regulation (GDPR) comes into force and brings with it a significant change to the UK's data protection laws. Additionally, the ICO (Information Commissioner's Office) will be empowered to impose fines of up to 4% of global revenue or 20 million euros for breaches of the new guidelines. As a result, those organisations affected by the Regulations need to work quickly to confirm that they understand, and can comply with, the new law.

1.2 Compliance with GDPR requires organisations to be able to understand and record what personal data they gather, why they gather it, how they handle it, where they hold it and how they share it. The data obtained should also be proportionate, kept up to date and accurate, and only held for as long as it is required. For many organisations, this will mean developing a raft of new processes and policies in order to ensure compliance. SPA and Police Scotland are also bound by the new Law Enforcement Directive (LED) which comes into effect on 6 May 2018. This relates to "the processing of personal data by the police and other criminal justice agencies for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data".

1.3 The Law Enforcement Directive contains six data protection principles which apply to personal data processed by a law enforcement agency. These are the requirements that:

- processing be lawful and fair;
- the purposes of processing be specified, explicit and legitimate;
- personal data be adequate, relevant and not excessive;
- personal data be accurate and kept up to date;
- personal data be kept no longer than is necessary; and
- personal data be processed in a secure manner.

1.4 It also sets out the rights of individuals over their data. These include:

- rights of access by the data subject to information about the data processing (including the legal basis for processing, the type of data

held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint);

- the right to rectification of inaccurate data and of erasure of data (or the restriction of its processing) where the processing of the data would infringe the data protection principles; and
- rights in relation to automated decision-making (that is, decision making that has not involved human intervention).
- It places restrictions on those rights, but only where necessary and proportionate in order to:

  - avoid obstructing an investigation or enquiry;
  - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security;
  - protect national security; and
  - protect the rights and freedoms of others.

1.5 The Information Commissioner's Office has produced a guidance document based on 12-Steps to achieving compliance with GDPR. This is the basis on which SPA and Police Scotland have sought to take forward GDPR and LED compliance.

1.6 These 12 steps are:

1. **Awareness -** You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.
2. **Information you hold -** You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
3. **Communicating privacy information -** You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
4. **Individuals' rights** - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests -** You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6. **Lawful basis for processing personal data** - You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
7. **Consent -** You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children -** You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
9. **Data breaches -** You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
10. **Data Protection by Design and Data Protection Impact Assessments -** You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
11. **Data Protection Officers** - You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
12. **International -** If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

1.7 A key element of GDPR compliance is ensuring that appropriate arrangements are in place to identify gaps in data management practices, policies etc. and developing a formal programme of work to address these.

1.8 Our audit sought to confirm the readiness of Police Scotland and SPA (including Forensic Services) for the introduction of the GDPR requirements in May 2018.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Separate management action plans and conclusions were produced for SPA and Police Scotland and a summary of each is provided below.

SPA

2.2 The SPA Information Management team has been allocated responsibility for data protection arrangements within both SPA Corporate as well as Forensic Services. The majority of personal data held within SPA is related to Forensic Services.

2.3 It was of concern to note that limited progress has been made by SPA in working towards compliance with the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED).

At the time of our audit work, a formal gap analysis had not been performed which clearly set out the actions necessary for achieving compliance by May 2018. A key reason for this has been lack of staff. Approval has been granted for recruitment of two additional members of staff to assist with GDPR compliance and actions arising from the consensual Data Protection audit by the ICO. In addition to this, approval for the recruitment of a Data Protection lawyer has been approved. Adverts for both of these positions will be published before the end of 2017. In the absence of an action plan which sets out staffing and skills requirements, we are unclear how SPA has determined that this level of staffing will be sufficient to address required actions.

2.4 In addition, SPA is seeking these staff at a time when such individuals are in high demand. As a result, there is a high risk that SPA will either take longer than anticipated to recruit staff or may not be able to recruit staff at all. We were also concerned to note that there is no contingency plan in place e.g. using a third party.

2.5 SPA should also manage the GDPR/LED compliance activity as a project. It is intended to operate it as a business-as-usual activity. By managing the activity as a project, SPA management will be able to have a better control framework. The project should include a Project Sponsor, Project Board, risks and issues logs and formal reporting to SPA senior management.

2.6 Our audit work has established that significant work needs to be undertaken by SPA to achieve compliance with GDPR and LED

requirements. If appropriately skilled staff are not recruited quickly it will be unlikely that SPA will achieve compliance by May 2018.

2.7 Our audit identified two “grade 4” (very high risk) and two “grade 3” (high risk) areas for improvement. All recommendations contained within the report have been accepted with action owners and timescales for completion assigned.

Police Scotland

2.8 Police Scotland have established a project to manage the necessary changes to the organisation require as a result of upcoming changes to data protection legislation. This project is scoped to focus on GDPR and the Law Enforcement Directive (LED), as well as improving the use of data within the organisation.

2.9 Police Scotland recognise that they will not be compliant with GDPR and LED by May 2018, however plan to have a compliant framework by this point and achieving operational compliance by December 2018. Whilst this is recognised by Police Scotland, a risk assessment has not yet been undertaken to identify those areas which will not be compliant by May 2018 and how risks will be managed in the intervening period. It will be important to demonstrate to the ICO that there has been appropriate risk management for those areas which are not compliant by May 2018. A formal project plan has been developed, based around the ICO’s 12-Steps guidance. At the time of our audit, the plan was high level in nature and does not include details of the tasks and activities that are necessary for achieving compliance. In addition, the staffing and skills needed to deliver the project plan had not been quantified at the time of our audit. Therefore, it was not possible to gain assurance that the additional staffing provided for the project will be sufficient to address all actions.

2.10 A key dependency for Police Scotland in achieving compliance by December 2018 is being able to rely on a derogation contained within the Law Enforcement Directive for what Police Scotland regard as ‘legacy systems’. The derogation states:

“By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.”

2.11 No formal work has yet been undertaken to define those ‘legacy systems’ that would be included within this approach. Furthermore,

justification has not been documented nor has there be any legal opinion sought to establish whether Police Scotland's interpretation of Directive is applicable (for individual or all systems). It is vital that this is resolved as soon as possible as, if Police Scotland's interpretation is partially or fully incorrect, this could have a significant impact on the project.

2.12 Our audit identified one "grade 4" (very high risk), three "grade 3" (high risk) and two "grade 2" (moderate risk) areas for improvement. All recommendations contained within the report have been accepted with action owners and timescales for completion assigned.

2.13 Next steps: We will follow up management responses contained within the report on a periodic basis to monitor progress being made towards implementing management actions.

3. FINANCIAL IMPLICATIONS

3.1 There are no financial implications in this report.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications associated with this paper.

5. LEGAL IMPLICATIONS

5.1 There are no further legal implications in this paper to those listed above.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no reputational implications associated with this paper.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications associated with this paper.

8. COMMUNITY IMPACT

8.1 There are no community implications associated with this paper.

9. EQUALITIES IMPLICATIONS

9.1 There are no equality implications associated with this paper.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environment implications associated with this paper.

RECOMMENDATIONS
Members are requested to note the GDPR readiness report.

Scottish Police Authority

Internal Audit Report 2017/18

GDPR Readiness

December 2017

Scott-Moncrieff
business advisers and accountants

Scottish Police Authority

Internal Audit Report 2017/18

GDPR Readiness

Audit Sponsor	*Key Contacts*	*Audit team*
Angela McLaren, Police Scotland *Tom Nelson, SPA Forensic Services* *Stephen Jones, SPA*	*Mark Lundie, Police Scotland* *Steven Meikle, Police Scotland* *Robin Johnston, SPA* *Lindsey Davie, SPA*	*Paul Kelly, IT Audit Director* *Scott Bannerman, IT Auditor* *Rachel Wilson IT Auditor*

Introduction

Background

On 25 May 2018, the EU General Data Protection Regulation (GDPR) comes into force and brings with it a significant change to the UK's data protection laws. Additionally, the ICO (Information Commissioner's Office) will be empowered to impose fines of up to 4% of global revenue or 20 million euros for breaches of the new guidelines. As a result, those organisations affected by the Regulations need to work quickly to confirm that they understand, and can comply with, the new law.

Compliance with GDPR requires organisations to be able to understand and record what personal data they gather, why they gather it, how they handle it, where they hold it and how they share it. The data obtained should also be proportionate, kept up to date and accurate, and only held for as long as it is required. For many organisations, this will mean developing a raft of new processes and policies in order to ensure compliance. SPA and Police Scotland are also bound by the new Law Enforcement Directive (LED) which comes into effect on 6 May 2018. This relates to "the processing of personal data by the police and other criminal justice agencies for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data".

The Law Enforcement Directive contains six data protection principles which apply to personal data processed by a law enforcement agency. These are the requirements that:

- processing be lawful and fair;
- the purposes of processing be specified, explicit and legitimate;
- personal data be adequate, relevant and not excessive;
- personal data be accurate and kept up to date;
- personal data be kept no longer than is necessary; and
- personal data be processed in a secure manner.

It also sets out the rights of individuals over their data. These include:

- rights of access by the data subject to information about the data processing (including the legal basis for processing, the type of data held, to whom the data has been disclosed, the period for which it will be held and the right to make a complaint);
- the right to rectification of inaccurate data and of erasure of data (or the restriction of its processing) where the processing of the data would infringe the data protection principles; and
- rights in relation to automated decision-making (that is, decision making that has not involved human intervention).
- It places restrictions on those rights, but only where necessary and proportionate in order to:
    - avoid obstructing an investigation or enquiry;
    - avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security;
    - protect national security; and protect the rights and freedoms of others.

The Information Commissioner's Office has produced a guidance document based on 12-Steps to achieving compliance with GDPR. This is the basis on which SPA and Police Scotland have sought to take forward GDPR and LED compliance.

These 12 steps are:

1. **Awareness -** You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.
2. **Information you hold -** You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
3. **Communicating privacy information -** You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
4. **Individuals' rights** - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests -** You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
6. **Lawful basis for processing personal data** - You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
7. **Consent -** You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children -** You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
9. **Data breaches -** You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
10. **Data Protection by Design and Data Protection Impact Assessments -** You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.
11. **Data Protection Officers** - You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
12. **International -** If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

A key element of GDPR compliance is ensuring that appropriate arrangements are in place to identify gaps in data management practices, policies etc. and developing a formal programme of work to address these.

Scope

The review sought to confirm the readiness of Police Scotland and SPA (including Forensic Services) for the introduction of the GDPR requirements in May 2018.

To allow management to more clearly understand the effectiveness of controls in each organisation (SPA and Police Scotland) subject to this audit, we have produced separate Summary of Findings and Management Action Plans.

Acknowledgements

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

SPA – Executive Summary

Conclusion

The SPA Information Management team has been allocated responsibility for data protection arrangements within both SPA Corporate as well as Forensic Services. The majority of personal data held within SPA is related to Forensic Services.

It was of concern to note that limited progress has been made by SPA in working towards compliance with the EU General Data Protection Regulation (GDPR) and Law Enforcement Directive (LED).

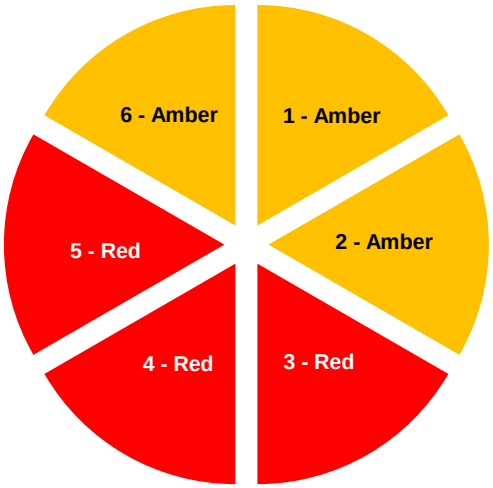
At the time of our audit work, a formal gap analysis had not been performed which clearly set out the actions necessary for achieving compliance by May 2018. A key reason for this has been lack of staff. Approval has been granted for recruitment of two additional members of staff to assist with GDPR compliance and actions arising from the consensual Data Protection audit by the ICO. In addition to this, approval for the recruitment of a Data Protection lawyer has been approved. Adverts for both of these positions will be published before the end of 2017. In the absence of an action plan which sets out staffing and skills requirements, we are unclear how SPA has determined that this level of staffing will be sufficient to address required actions.

In addition, SPA is seeking these staff at a time when such individuals are in high demand. As a result, there is a high risk that SPA will either take longer than anticipated to recruit staff or may not be able to recruit staff at all. We were also concerned to note that there is no contingency plan in place e.g. using a third party.

SPA should also manage the GDPR/LED compliance activity as a project. It is intended to operate it as a business-as-usual activity. By managing the activity as a project, SPA management will be able to have a better control framework. The project should include a Project Sponsor, Project Board, risks and issues logs and formal reporting to SPA senior management.

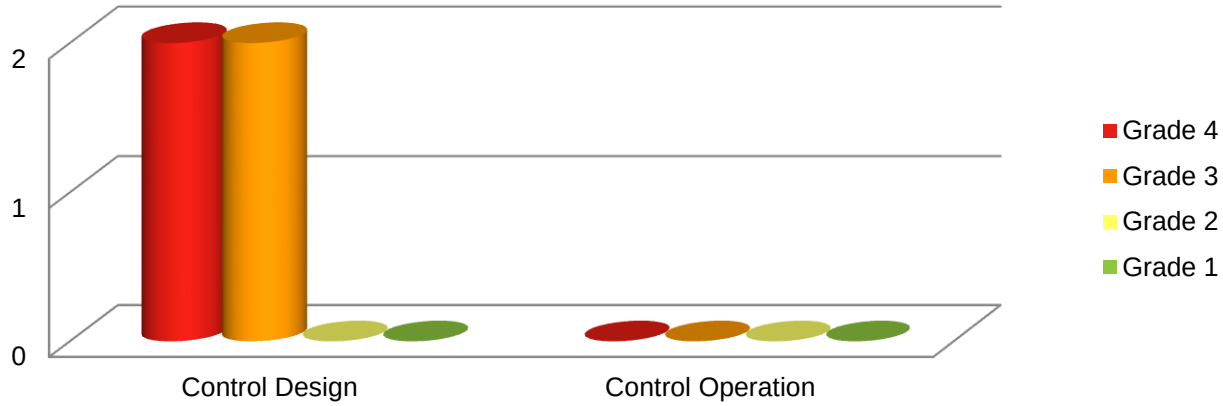
Our audit work has established that significant work needs to be undertaken by SPA to achieve compliance with GDPR and LED requirements. If appropriately skilled staff are not recruited quickly it will be unlikely that SPA will achieve compliance by May 2018.

Control assessment



- 1. A gap analysis has been conducted and documented to identify where current personal data management policies, practices and procedures are not consistent with the GDPR.
- 2. Action plans have been developed to address all identified gaps.
- 3. Action plans contain timescales for completion and responsibilities.
- 4. Appropriate resources are assigned to support achievement of action plans.
- 5. There is adequate governance to monitor progress in delivering action plans.
- 6. Plans are in place to ensure all relevant staff are made aware of the impact of GDPR and their role in supporting compliance.

Improvement actions by type and priority



Four improvement actions have been identified from this review, all of which relates to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Areas for improvement

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

- As a matter of urgency, SPA needs to develop a detailed action plan which sets out those tasks and activities that will be necessary to achieve compliance with GDPR and LED. It will also be necessary to assign action owners and completion dates. In doing so, SPA will need to quantify the level of staffing needed to address actions as well as the associated skills. Once this is complete, management should assess whether the planned staffing levels are sufficient.

- There is a need for a formal contingency plan to be developed in the event that SPA experiences delays in recruiting the approved additional staff. This should include investigation of using third parties to support delivery.

- SPA should manage GDPR/LED compliance as a project rather than a business as usual activity. This is a highly important initiative which, if not managed effectively, could result in significant financial penalties and reputational damage to the organisation. The project should include the nomination of a Project Sponsor along with the creation of a Project Board which meets regularly. The project should also include creation and maintenance of a risks and issues logs as well as formal reporting of progress to SPA senior management.

- There is a need to develop plans for training and awareness on GDPR and LED.

These are further discussed in the Management Action Plan below.

SPA - Management Action Plan

Control Objective 1: A gap analysis has been conducted and documented to identify where current personal data management policies, practices and procedures are not consistent with the GDPR.

Amber

Control Objective 2: Action plans have been developed to address all identified gaps.

Amber

1.1 Formal Gap Analysis and Action Plan

SPA has not developed a formal action plan to address gaps in compliance with the GDPR. Our audit work identified that SPA is working from two task lists. The first list contained the recommendations from an Information Commissioner's Office (ICO) audit against the Data Protection Act 1998. The second is the internal assessment against the GDPR which was based upon the ICO's 12-Steps guidance.

No action has been taken to develop a coherent action plan which identifies all tasks necessary to achieve compliance with the GDPR and Law Enforcement Directive (LED). We also identified that there has not been any work undertaken to consolidate and/or rationalise those tasks that are set out within these two lists or to establish the people requirement to complete the actions.

Risk

Without a formal, documented gap analysis, there is a risk that SPA does not have a clear indication of those areas where action is required to achieve compliance with the GDPR and LED. This could result in high priority actions not being identified and addressed.

By maintaining separate task lists, there is a risk that SPA will duplicate efforts and/or not realise synergies. This could result in scarce people resource being tasked to actions which add little or no value.

Recommendation

We recommend that a formal gap analysis is produced for SPA. This should identify all actions necessary to achieve compliance with the GDPR and LED. In developing this action plan, management should review the current tasks lists to confirm that all relevant recommendations from the ICO and internal assessment are being addressed.

Once this is completed, SPA should develop a detailed project plan which lists all actions, the timescales for their completion, action owners and people requirements to deliver them.

Management Action

Grade 3 (Design)

Agreed.

SPA has developed an action plan highlighting the key areas where additional work is required for GDPR compliance and is actively progressing these actions. A programme board approach has been initiated and will commence in January 2018 to review the deliverables, timescales and compliance/dates.

Recruitment to support the delivery has commenced, with sifting of the GDPR officer role concluding on the 15th January with interviews concluding in January 2018.

Following the implementation of the programme governance, a continual review cycle will be put in place to ensure management is overseeing the delivery of the work streams.

Action owner: Lindsey Davie **Due date:** March 2018

Control Objective 3: Action plans contain timescales for completion and responsibilities.

Red

Control Objective 4: Appropriate resources are assigned to support achievement of action plans.

Red

3.1 Timescales and Responsibilities

At the time of our review, SPA had yet to assign completion dates and responsibilities to the actions necessary to achieve compliance with the incoming GDPR and LED. We were informed that this was due to a lack of staff within the organisation to assign the tasks to. By default, responsibility would lie with the Head of Information Management.

When conducting our audit work, there were two members of SPA staff working on GDPR and LED compliance at SPA. These staff are performing this role in addition to their day jobs. As a result, limited progress has been made.

Approval has been given to recruit two temporary members of staff to assist with completion of actions, and a Data Protection Lawyer to advise on the relationship between Police Scotland and SPA in terms of information transfer. As an action plan has not yet been developed, it is unclear how SPA identified that this was the correct level of staff to address requirements.

We were informed that if recruitment was to take longer than anticipated, there is no secondary plan and a decision would have to be taken whether to prioritise day to day compliance activities or GDPR compliance activities.

Risk

If actions are not assigned owners, there is an increased likelihood that they will not be progressed in line with expectations. In addition, if timescales are not assigned and monitored for actions, there will be no understanding of whether the tasks will be completed in time for the new legislation coming into force. This increases the risk of SPA being subject to a severe financial penalty.

There is a significant risk that SPA will not be able to or will experience delays in recruiting appropriately skilled data protection specialists due to the high market demand. This will result in SPA not being compliant with GDPR in May 2018 and increases the risks of severe financial penalties and reputational damage.

Recommendation

We recommend that once an action plan has been developed (as per MAP1.1), management make a formal assessment of the people resources required to deliver it. If there is any additional people requirement, this should be escalated as soon as possible to senior management for review and approval.

In light of the current high market demand for data protection specialists, SPA management should develop formal contingency arrangements in the event that the additional staff cannot be recruited in line with expected timescales. This should include consideration of partnering with a third party who would be able to provide staffing for a fixed period.

Management Action

Grade 4 (Design)

Agreed.

SPA will consider all other resource support options, including sourcing support from other government departments, recruitment agencies and if necessary consultancy. However, the recruitment plan in place to date has been effective.

Action owner: Lindsey Davie **Due date:** March 2018

Control Objective 5: There is adequate governance to monitor progress in delivering action plans.

Red

5.1 Progress Monitoring

It was identified that GDPR and LED compliance activities are being taken forward as a business as usual activity within SPA rather than a project. As such there is no formal governance structure to oversee progress towards compliance.

Additionally, due to the lack of a detailed action plan and project framework, there are no established metrics to allow management to monitor progress in achieving compliance.

Risk

Without managing GDPR and LED compliance as a project, SPA management may not be able to fully assess progress as well as risks and issues that could impact on the ability of the organisation to achieve compliance by May 2018.

Recommendation

We recommend that GDPR and LED compliance is managed as a project within SPA. This should include the creation of a formal project framework which includes a Project Sponsor (member of the Senior Management Group) being assigned to the project, the creation of a project board as well as the creation and maintenance of risk and issues logs. The Project Board should meet on a regular basis. Given the timescales to implementation this should be at least monthly with highlight reports being submitted to the SPA Senior Management Group so that they have a clear understanding of progress and how risks and issue are being managed.

Management Action

Grade 4 (Design)

Agreed, and the senior management team have commissioned this. The programme board, and associated work streams will be implemented in January 2018.

Action owner: Lindsey Davie **Due date:** March 2018

Control Objective 6: Plans are in place to ensure all relevant staff are made aware of the impact of GDPR and their role in supporting compliance.

Amber

6.1 Training

A decision has not yet been made regarding the format of training to be provided to staff at SPA in relation to GDPR and LED compliance. Up until this point, data protection training has been delivered through face-to-face sessions; however there is insufficient capacity to provide this type of training to all SPA staff at present and on an annual basis as mandated by GDPR.

Risk

By not providing appropriate training to staff in relation to GDPR and LED requirements, there is risk that staff will not be aware of their role and responsibilities in protecting personal data. This could result in operating practices and staff behaviours being inconsistent with policy and legislative requirements, increasing the risk of a breach of personal data. If a breach was to occur this could result in a risk of significant financial penalty and reputational damage.

Recommendation

We recommend that training and awareness requirements are included within the GDPR and LED action plan. Training should be provided through face-to-face sessions or through the use of e-learning tools. In addition, there should be regular awareness raising campaigns conducted to highlight the importance of the requirements of GDPR and LED. This should include, for example, email communications, notice board posters, features on the intranet etc.

Management Action

Grade 3 (Design)

Agreed.

This is the first step on the ICO's 12 step plan and SPA is aware of the requirement as per Section 1, item (e) of our plan. We have secured approval to look at an electronic medium to deliver training. We will also be working with Police Scotland on any possible shared solution, and seek to undertake training in Q4 with all staff

Action owner: Linsev Davie **Due date:** March 2018

Police Scotland – Executive Summary

Conclusion

Police Scotland have established a project to manage the necessary changes to the organisation require as a result of upcoming changes to data protection legislation. This project is scoped to focus on GDPR and the Law Enforcement Directive (LED), as well as improving the use of data within the organisation.

Police Scotland recognise that they will not be compliant with GDPR and LED by May 2018, however plan to have a compliant framework by this point and achieving operational compliance by December 2018. Whilst this is recognised by Police Scotland, a risk assessment has not yet been undertaken to identify those areas which will not be compliant by May 2018 and how risks will be managed in the intervening period. It will be important to demonstrate to the ICO that there has been appropriate risk management for those areas which are not compliant by May 2018.

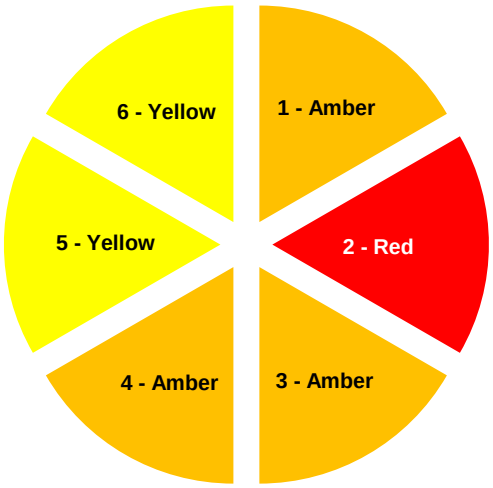
A formal project plan has been developed, based around the ICO's 12-Steps guidance. At the time of our audit, the plan was high level in nature and does not include details of the tasks and activities that are necessary for achieving compliance. In addition, the staffing and skills needed to deliver the project plan had not been quantified at the time of our audit. Therefore, it was not possible to gain assurance that the additional staffing provided for the project will be sufficient to address all actions.

A key dependency for Police Scotland in achieving compliance by December 2018 is being able to rely on a derogation contained within the Law Enforcement Directive for what Police Scotland regard as 'legacy systems'. The derogation states:

"By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023."

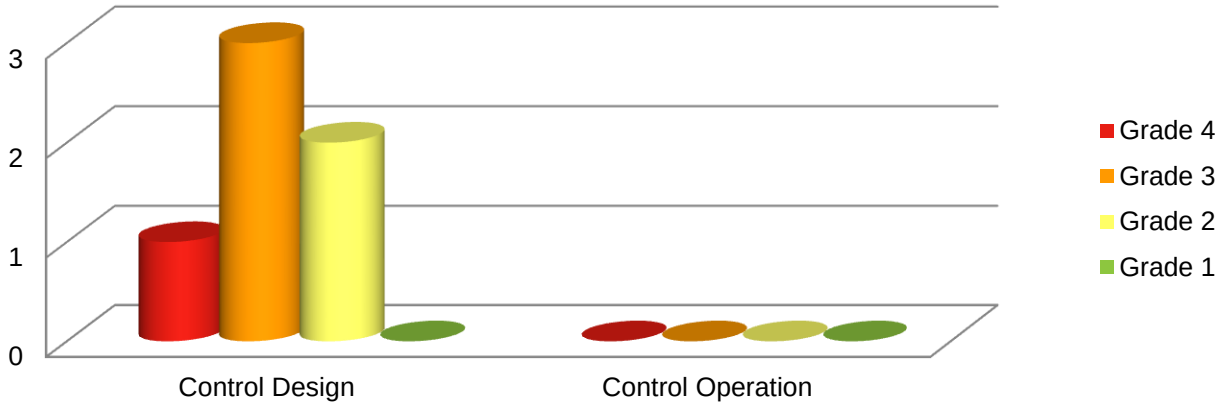
No formal work has yet been undertaken to define those 'legacy systems' that would be included within this approach. Furthermore, justification has not been documented nor has there be any legal opinion sought to establish whether Police Scotland's interpretation of Directive is applicable (for individual or all systems). It is vital that this is resolved as soon as possible as, if Police Scotland's interpretation is partially or fully incorrect, this could have a significant impact on the project.

Control assessment



- 1. A gap analysis has been conducted and documented to identify where current personal data management policies, practices and procedures are not consistent with the GDPR.
- 2. Action plans have been developed to address all identified gaps.
- 3. Action plans contain timescales for completion and responsibilities.
- 4. Appropriate resources are assigned to support achievement of action plans.
- 5. There is adequate governance to monitor progress in delivering action plans.
- 6. Plans are in place to ensure all relevant staff are made aware of the impact of GDPR and their role in supporting compliance.

Improvement actions by type and priority



Six improvement actions have been identified from this review, all of which relate to the design of controls themselves. See Appendix A for definitions of colour coding.

Key findings

Areas for improvement

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

- There is a need for Police Scotland to develop a detailed project plan which sets out all tasks and activities that will need to be addressed to achieve compliance with GDPR/LED. The staffing and skills needed to address the project plan has not yet been defined. As a result, there is a need for an exercise to be undertaken to quantify the staffing requirement as well as the skills needed. Furthermore, there is a need for an exercise to be undertaken to identify whether the current additional staffing provided has the capacity and capability to address GDPR/LED compliance requirements.

- An information audit had only recently commenced at the time of our audit. The purpose of this is to create Information Asset Registers. Understanding personal data held and how it is needs to be protected is a key element of performing GDPR gap analyses. It is expected that the information audit will be completed by December 2018 meaning that there could be significant additional tasks and activities having to be added to the project plan as information audits are completed.

- Police Scotland aim to rely upon a derogation contained within the Law Enforcement Directive in relation to addressing personal data contained within 'legacy systems'. There has not been any exercise undertaken which sets out the justification for the proposed approach for individual systems. In addition, legal opinion has not been sought to establish the veracity of Police Scotland's proposed approach.

- At the time of our audit, governance arrangements were in the process of being established with the intention being that the project team report into the Information Governance Group (IGG). The IGG is meeting for the first time on 21 December 2017 at which time it will be agreeing its remit. It will be important for management to monitor the effectiveness of governance arrangements over the project to confirm that progress is being made and that risks and issues are being addressed in a timely manner.

These are further discussed in the Management Action Plan below.

Police Scotland - Management Action Plan

Control Objective 1: A gap analysis has been conducted and documented to identify where current personal data management policies, practices and procedures are not consistent with the GDPR.

Amber

1.1 Gap analysis and Information Asset registers

During 2016, Police Scotland was subject to a consensual audit by the ICO. This identified compliance gaps against the Data Protection Act 1998. Police Scotland has subsequently taken the ICO's 12-Steps guidance to set out the target environment to be established.

An exercise has been undertaken to compare the results of the ICO audit and the gap analysis against the 12-Steps guidance to establish a project plan. This project plan is broken down into the twelve areas detailed in the ICO's guidance.

However, a key element of the gap analysis is creating Information Asset Registers (IARs) to allow understanding of personal data held and how it needs to be protected. At the time of our audit, work on creating IARs had only recently started and this process is due to be completed by December 2018.

Risk

There is a risk that, without having conducted the information audit (to create IARs), the gap analysis may not have identified all areas where compliance issues need to be addressed. This could result in significant additional work having to be undertaken as part of the project.

Recommendation

We recommend that management monitor outputs from information audits so that any additional project tasks and activities are identified and assessed as soon as possible. If any changes are necessary the impact of these should be formally assessed to establish whether they affect delivery timescales and staffing needs.

Management Action

Grade 3 (Design)

Agreed.

The Project Team will establish a methodology to assess the outcome of each audit to ensure any additional project tasks and activities which are required are addressed. These will be captured in 'issue logs' for progression. The methodology will be established by due date.

Action owner: SRO **Due date:** 1 February 2018

Control Objective 2: Action plans have been developed to address all identified gaps.

Red

2.1 Legacy Systems

It was observed that tasks listed in the project plan are high level in nature An example of this was in relation to actions on legacy systems.

At the time of our audit, work had still to be undertaken to consider how Police Scotland would address data held within legacy systems.

The aim is to commence the creation of a register of 'legacy systems' in January 2018. During the course of our audit work, it was the stated that it was intended to rely on a derogation detailed in Article 63, Paragraph 2 of the Directive, as follows:,

"*By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.*"

It is intended that Police Scotland will rely on this derogation until legacy systems can be either decommissioned or brought up to a compliant level.

Although Police Scotland believe that this derogation is applicable to a number of legacy systems, there has not been any formal exercise conducted which lists those systems which would fall within the scope of this approach and the justification for this. Furthermore, there has not been any legal opinion sought to establish the veracity of this proposed approach.

It is expected that this information will be obtained as part of the work that has recently commenced on the creation of Information Asset Register. The task of populating all Information Asset Registers is not due to be completed by December 2018.

Risk

There is a risk that, without formal opinion being sought on the applicability of the derogation, Police Scotland's interpretation of the derogation may be incorrect. If this is the case, this will have significant negative impact on the overall GDPR/LED project.

Recommendation

We recommend that action is taken as a matter of urgency to identify those 'legacy systems' where it is proposed that the derogation will be applicable. Justification for the derogation should be formally documented and legal opinion sought to confirm the veracity of Police Scotland's proposed approach.

If the Police Scotland position is upheld, a plan should be developed detailing the options available to bring these systems up to the standards required by legislation, whether this be by replacement or redevelopment.

If the Police Scotland position is not upheld (either in full or in part), a risk and impact assessment on the project plan should be conducted. This should consider what actions will need to be accelerated/prioritised in order that risks relating to legacy systems are appropriately managed.

Management Action

Grade 4 (Design)

Agreed.

The systems will be identified as part of the audit schedule. The assessment methodology mentioned in paragraph above should identify these.

Police Scotland will seek legal opinion and if upheld we will develop a plan to address the systems. If the position is not upheld a risk and impact assessment will be conducted to allow for appropriate action.

Action owner: SRO **Due date:** 1 May 2018

Control Objective 3: Action plans contain timescales for completion and responsibilities.

Amber

3.1 Compliance by May 2018

It was also identified that the project is being approached in two stages. The first stage has an intended completion date of 1 May 2018, and focuses on the implementation of a compliant framework of policies and procedures. Phase two is planned to be completed in December 2018 and focuses on the organisation being operationally compliant.

A number of tasks defined within the project plan have completion dates of December 2018, despite these being integral to compliance with GDPR. It is not clear what aspects of these tasks will be completed by the deadline and therefore to what extent Police Scotland will be compliant by May 2018. In addition, a risk assessment has not yet been undertaken to identify those areas which will not be compliant by May 2018 and how risks will be managed in the intervening period.

Risk

There is a risk that by not being compliant with Data Protection legislation by May 2018 that Police Scotland are exposed to severe financial and reputational damage through fines and adverse publicity.

Recommendation

We recommend that, where possible, areas of the Data Protection Reform project related to personal data are prioritised over operational data areas in order to increase the level of compliance by May 2018.

Additionally, where it has been decided that compliance will not be achieved by May 2018, a detailed plan of how this will be rectified should be produced as a potential mitigation in the event that Police Scotland is found in breach of the legislation. Management should also document formal risk assessments for each area where it is expected where compliance will not be achieved by May 2018.

Grade 3 (Design)

Management Action

Agreed.

Business areas which process the highest volumes of personal data are being prioritised over operational areas where appropriate. This has already been reflected in the Information Asset scheduling.

Areas which will not be complaint will be subject to a Risk Assessment and required to detail their plans to move towards compliance.

Action owner: SRO **Due date:** 1 May 2018

Control Objective 4: Appropriate resources are assigned to support achievement of action plans.

Amber

4.1 Staffing requirements

As mentioned in 2.1, an action plan has been developed by Police Scotland which is based around the ICO's 12-Steps guidance.

Our review identified that, whilst a project plan has been developed, this is high level in nature. We noted that it does not include a breakdown of the people and skills needed to fulfil all tasks and activities. As such detailed people resourcing requirement has not yet been defined.

Without this we have not been able to confirm how Police Scotland has quantified the additional staffing requirement to address the action plan and meet GDPR/LED requirements.

Risk

There is a risk that, without a project plan which sets out people resource requirements against all tasks and activities, Police Scotland will not be able to confirm that they have the correct skills and people available at critical stages of the project. This could result in delays in and compliance requirements not being fulfilled in line with deadlines.

Recommendation

We recommend that an exercise is undertaken to populate the project plan with all tasks and activities that are necessary to achieve compliance by May 2018. This should include an assessment of the people resource needed to deliver each task and, where appropriate, any specialist skills needed to undertake the task activity.

Once this exercise is complete, a review should be performed to confirm whether there is sufficient people and skills available to address requirements.

Management Action

Grade 3 (Design)

Agreed.

In early January 2018 further work will be undertaken to review and populate the existing detailed project plan which will take into account the resources required to deliver each activity.

Action owner: SRO **Due date:** 1 February 2018

Control Objective 5: There is adequate governance to monitor progress in delivering action plans.

Yellow

5.1 Project Governance

During our review, we were informed that fortnightly project team meetings would be held, and that the project would report to an Information Governance Board (IGB).

However, the IGG is only due to have its first meeting on 21 December 2017, at which point the remit of the IGG is to be discussed and agreed.

Additionally, while the inaugural project team meeting is believed to have taken place in early December, we were unable to obtain any formal output from this.

Risk

Without a forum providing oversight and challenge to project progress, there is a risk that management cannot be accurately identify the current project position cannot gain assurance regarding the likelihood of being compliant with legislation by May 2018.

Recommendation

We recommend that all formal project meetings are recorded and that a regular report is provided to the IGG. once it is formally established to allow progress to be tracked. This will allow for regular review of challenge. Mechanisms should also be established which allows for any significant risks or issues to be escalated in a timely manner to allow for action to be taken.

Management Action

Grade 2 (Design)

Agreed.

Project Meetings are in place and the outcomes are recorded by means of an Action and Decision Log. Significant risks and updates will be escalated via the SRO and Deputy SRO to the Force Executive via existing governance structures.

Action owner: SRO **Due date:** 1 February 2018

Control Objective 6: Plans are in place to ensure all relevant staff are made aware of the impact of GDPR and their role in supporting compliance.

Yellow

6.1 Communications Plan

Single Points of Contact (SPOC) were identified and briefings were conducted in early December to brief relevant individuals on their responsibilities with regards to data protection. Personnel who own tasks detailed in the project plan have been briefed and are aware of their responsibilities.

However at the time of our review a full communications plan was not yet in place. This was due to be completed by the end of December 2017.

Risk

There is a risk that all relevant parties are not made aware of their role and responsibilities in relation to GDPR in a timely manner. This could result in delays in progressing tasks and activities within the project plan.

Recommendation

We recommend management develop and implement the proposed communications plan for GDPR and LED as soon as is practical. The success of the communications plan should be subject to monitoring by the project team and any remedial action taken to address any instances where clarity is required in relation to roles and responsibilities.

Grade 2 (Design)

Management Action

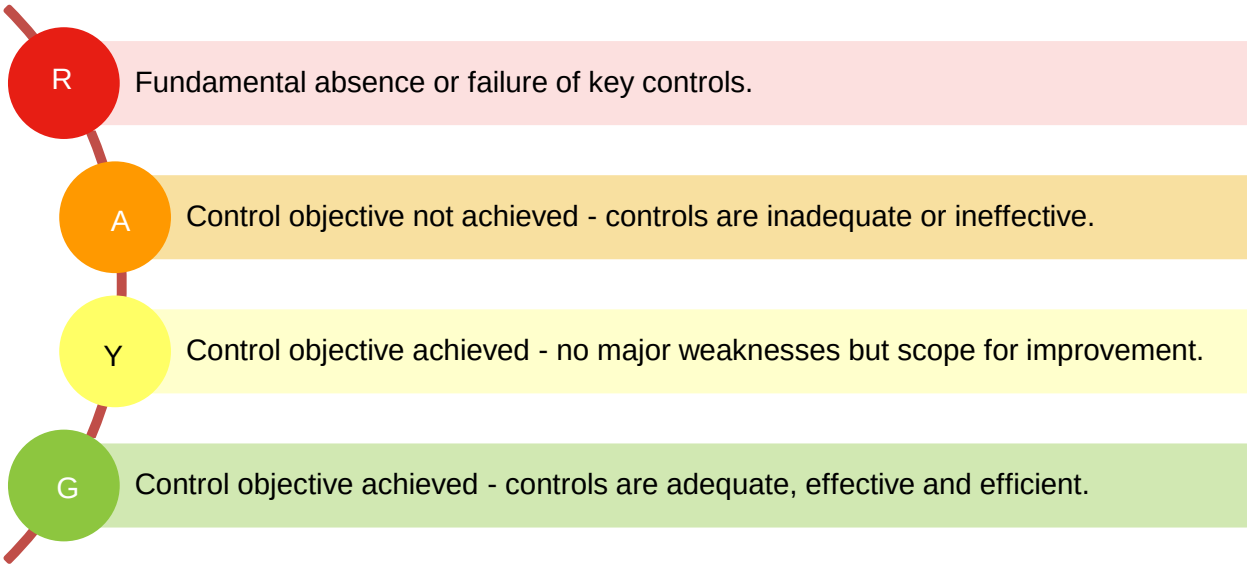
Agreed.

Communication plan is in place and subject to continual review via Project Board to ensure understanding across the organisation.

Action owner: SRO **Due date:** Completed

Appendix A – Definitions

Control assessments



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.