SCOTTISH POLICE AUTHORITY

Meeting	**Audit Committee**
Date	**24 July 2018**
Location	**Pacific Quay, Glasgow**
Title of Paper	**Internal Risk Management Report**
Item Number	**5.6**
Presented By	**Helen Berry, Director, Scott-Moncrieff**
Recommendation to Members	**Members are requested to note the report**
Appendix Attached	**Internal Audit Risk Management Report**

PURPOSE

This paper presents our final report on the review of the draft Risk Management Framework.

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

The paper is submitted for noting.

1. BACKGROUND

1.1 Risk is an inseparable part of any organisation which affects its operations and activities. Successful organisations are those that have robust risk management procedures to effectively manage and treat those risks before they impair the organisation's reputation and its ability to operate.

Risk management should be a continuously evolving process which is embedded within the organisation's culture. The management of risk at strategic, programme and operational levels needs to be integrated to ensure the levels of activity support each other. In this way, the risk management strategy of the organisation will be led from the top and embedded in the normal working routines and activities of the organisation.

2. FURTHER DETAIL ON THE REPORT TOPIC

2.1 Scott-Moncrieff has been requested to undertake a desktop review of the Draft Police Scotland Risk Management Framework. As part of this review, we have considered the risk management principles contained within the following guidelines and publications:

- 2018 ISO 31000 Risk Management Standard
- Scottish Public Finance Manual (SPFM): Risk Management

Police Scotland advised that the section on Risk Appetite within the Draft Risk Management Framework is still under development and, as such, this section has been excluded from our review. In addition, as the Framework is currently in draft, we have not assessed the application of risk management processes within Police Scotland.

The report contains four minor improvement opportunities which, if implemented, will strengthen the Risk Management Framework. These have all been accepted by management and the Draft Risk Management Framework has been updated accordingly.

Next steps: We will follow up management responses contained within the report during the Q1 Follow Up process to confirm that all improvement opportunities have been actioned.

3. FINANCIAL IMPLICATIONS

3.1 There are no financial implications arising as a direct result of this report.

4. PERSONNEL IMPLICATIONS

4.1 There are no personnel implications associated with this report.

5. LEGAL IMPLICATIONS

5.1 There are no legal implications associated with this report.

6. REPUTATIONAL IMPLICATIONS

6.1 There are no reputational implications arising from with report.

7. SOCIAL IMPLICATIONS

7.1 There are no social implications directly associated with this report

8. COMMUNITY IMPACT

8.1 There are no community impact implications directly associated with this report.

9. EQUALITIES IMPLICATIONS

9.1 There are no equalities implications directly associated with this report.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no environmental implications associated with this report.

RECOMMENDATIONS
Members are requested to note the report.

Scottish Police Authority

Draft Risk Management Framework Review

July 2018

Scott-Moncrieff
business advisers and accountants

Scottish Police Authority

Draft Risk Management Framework Review

Executive Summary

Introduction

Risk is an inseparable part of any organisation which affects its operations and activities. Successful organisations are those that have robust risk management procedures to effectively manage and treat those risks before they impair the organisation's reputation and its ability to operate.

Risk management should be a continuously evolving process which is embedded within the organisation's culture. The management of risk at strategic, programme and operational levels needs to be integrated to ensure the levels of activity support each other. In this way, the risk management strategy of the organisation will be led from the top and embedded in the normal working routines and activities of the organisation.

There are many recommended approaches to risk management with a wide variety of published standards and risk management frameworks.

Scope of Review

Scott-Moncrieff has been requested to undertake a desktop review of the Draft Police Scotland Risk Management Framework. As part of this review, we have considered the risk management principles contained within the following guidelines and publications:

- 2018 ISO 31000 Risk Management Standard
- Scottish Public Finance Manual (SPFM): Risk Management

Police Scotland advised that the section on Risk Appetite within the Draft Risk Management Framework is still under development and, as such, this section has been excluded from our review. In addition, as the Framework is currently in draft, we have not assessed the application of risk management processes within Police Scotland.

Conclusion

We have reviewed Police Scotland's Draft Risk Management Framework and have identified that the framework appears to be in line with ISO 31000 Risk Management Standard and SPFM Risk Management Guidance.

We have highlighted three minor areas of improvement where the Draft Risk Management Framework could be strengthened and identified some additional factors for management to consider as part of the implementation of the Framework, once it is finalised and approved.

Acknowledgements

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

Main Findings

We have reviewed the Police Scotland Draft Risk Management Framework (the Framework) against publicly available standards and guidance and have identified where the Framework appears to be in line with ISO 31000 Risk Management Standard and SPFM Risk Management Guidance.

The Framework contains the following elements:

- An Executive Foreword (yet to be completed);
- An introduction to risk and risk management;
- A risk management policy;
- A section on risk appetite; (this section has been excluded from our review as noted above);
- An introduction to risk culture and risk maturity;
- A section on risk architecture including:
  - governance and reporting arrangements
  - risk escalation policy; and
  - roles and responsibilities in relation to risk management;
- A section on risk guidance including the ISO 31000 risk management process; and
- A risk glossary

We have noted the following areas where the Framework could be strengthened:

- Within Section 6.2, management should consider providing further guidance on the decision making process at the DCC/DCO management boards for determining whether specific risks should be further escalated to the Organisational Risk Register and therefore the Audit and Risk Board and the SPA.
- Within Section 6.2, management should consider clarifying whether it is the untreated or current score that is used to determine whether the risk requires to be escalated for further monitoring and oversight.
- Within Section 6.3, management should consider including a description of the role / responsibilities of SPA and the SPA Interim Chief Officer (as Accountable Officer) in relation to management of Police Scotland risks.
- Management should consider updating Section 7.4 to include an example of a risk within the Framework which encompasses the following elements:
  - Identification of the risk including cause and impact
  - The untreated score determining the likelihood and impact
  - The identified controls, mitigation and contingency plans that have been implemented to address the untreated risk
  - The current score determining the likelihood and impact.

Next steps

We note that, once the Framework is implemented, Police Scotland plans to assess its risk maturity on an ongoing, regular basis using the Audit Scotland Best Value Toolkit for Risk Management. This will help Police Scotland to assess their current maturity and identify any improvements that are necessary to move the Risk Management Framework into better or advanced practice.

In order to successfully implement the Framework, we recommend management considers the following actions:

- Develop an implementation plan for the successful integration of the Risk Management Framework including the identification of actions, action owners and deadlines for implementation.
- Develop Risk Management Framework training materials which encompass the new process, policies and procedures.
- Ensure that all affected staff members (Risk Champions, Risk Leads, Risk Owners, Divisional Commanders / Heads of Departments, Risk Management Officers, Enterprise Risk Managers, DCC / DCO Tier 2 Boards, Audit and Risk Board, Force Executive and the Chief Constable) undertake this training prior to the implementation of the Framework.

2018 ISO 31000 Risk Management Standard

Framework assessment against ISO 31000

The ISO 31000 guidelines provide a statement of risk management principles. The eight principles are described below:

- **Framework and processes should be customised and proportionate.**
- **Appropriate and timely involvement of stakeholders is necessary.**
- **Structured and comprehensive approach is required.**
- **Risk management is an integral part of all organisational activities.**
- **Risk management anticipates, detects, acknowledges and responds to changes.**
- **Risk management explicitly considers any limitations of available information.**
- **Human and cultural factors influence all aspects of risk management.**
- **Risk management is continually improved through learning and experience.**

The first five principals provide guidance on how a risk management process should be designed and principles six, seven and eight relate to the operation of the risk management process. These latter principles confirm that the best information available should be used; human and cultural factors should be considered; and the risk management arrangements should ensure continual improvement. Given the draft status of the Framework, we have focused our review on the first five principles.

We assessed the Framework against the first five principles of the ISO 31000 Risk Management Standard, and concluded that the Framework follows good practice within the Standard. Our assessment against each of these principles is as follows:

1. Framework and processes should be customised and proportionate.

The Framework includes a statement regarding the importance of an effective risk management policy which reflects Police Scotland's strategic focus on "Keeping People Safe" and the responsibilities that the organisation faces in the public sector in terms of achieving best value and ensuring transparency.

While the Risk Appetite section has been excluded from this review, there is evidence that the Framework has been customised to reflect Police Scotland's risk categories namely Finance, Legal, H&S, Wellbeing, Service Delivery, Public Confidence and Change. The risk categories appear to be proportionate to the range of challenges facing Police Scotland.

2. Appropriate and timely involvement of stakeholders is necessary.

The Risk Management Policy within the Framework notes that one of the objectives of the risk management practices is to provide assurance to internal and external boards and stakeholders. The Framework stresses the importance of communicating with SPA and other stakeholders to allow effective scrutiny and provide assurance that the risk profile is effectively managed.

Additionally, the Framework stresses the importance of consulting with and receiving information from other departments and stakeholders to inform the management of the risks.

3. Structured and comprehensive approach is required.

The Framework sets out a structured, comprehensive approach to risk management with clearly articulated governance and reporting structures, risk escalation processes and documented roles and responsibilities across the organisation.

Additionally, the Framework contains the ISO 31000 Risk Management Process model which is designed to ensure that risk management is a dynamic process, with frequent review and monitoring to ensure the risks captured reflect the current profile of the organisation.

4. Risk management is an integral part of all organisational activities.

The Framework notes that "*its core objective is to achieve a consistent and effective application of risk management and allow it to be embedded into all core processes, forming part of the day-to-day management processes across the organisation. Risk management, when executed effectively, should add value by supporting day-to-day activities as opposed to being seen as a separate, self-contained process and this Framework supports this approach*".

Additionally, the Risk Management Policy within the Framework notes that the objectives of the risk management practices are to:

- Fully implement and embed Enterprise Risk Management across the organisation to allow an interrelated risk portfolio to be understood and managed;
- Improve risk-based decision-making and allow for better prioritisation pf resources;
- Ensure that the Risk Management Framework is understood and implemented by all staff with risk management responsibilities across all divisions and business areas.
- Improve awareness of risk management across the organisation, integrating it into the culture of Police Scotland.

5. Risk management anticipates, detects, acknowledges and responds to changes.

The Framework contains the ISO 31000 Risk Management Process model which represents a continuous cycle starting with the establishing the context in which the organisation is assessing the risks and the identification of the risks within that context.

Police Scotland has also identified nine ways in which risks can be identified including Risk Identification Workshops which will be undertaken on an annual basis in each department and division and facilitated by the Risk Management Team.

Scottish Public Finance Manual (SPFM) Risk Management Guidance

Framework assessment against SPFM

The Scottish Public Finance Manual gives guidance on the basic principles of risk management and is aimed at all organisations to which the SPFM is directly applicable. There are six elements within the SPFM guidance that are relevant to the review of the Police Scotland Framework:

- **Identifying the risk**
- **Ownership of the risk**
- **Assessing the risk**
- **Risk appetite**
- **Response to risk**
- **Reviewing and reporting**

Appendix 1 includes extracts from the SPFM that provide additional detail of the required activities under each of these principles. We assessed the Police Scotland Draft Risk Management Framework against the SPFM Risk Management guidance and found that, in general, the Framework is consistent with the guidance.

We noted a small number of minor improvement areas that management may wish to consider, which are set out in the remainder of this section, alongside details of our assessment of the Framework against each of the SPFM principles:

1. Identifying the risk

The Framework contains the ISO 31000 Risk Management Process model which is designed to demonstrate that risk management is a dynamic process, with frequent review and monitoring to ensure the risks captured reflect the current profile of the organisation.

Section 7.2 within the Framework details guidance on how risks should be identified across the organisation. This provides information on how the organisation should establish the context within which they are assessing risk by considering their individual strategic and operational objectives.

The Framework contains some useful prompts for users to consider during the risk identification process and lists a number of methods that can be used to identify risks such as:

Focused Identification Methods	Other Identification Opportunities
• Risk Identification Workshops • Risk Questionnaires • Review & refresh of existing risk registers • Interviews	• Horizon scanning • Board meetings/working groups/SMT meetings • Audit & scrutiny reports • Performance data • Risk Management Training Course

The Framework notes that the Risk Identification Workshops will be held annually and will be facilitated by the Risk Management Team. It notes in section 7.3 the importance of establishing cause, risk and impact to ensure that the risk can be effectively managed and provides examples of effective risk descriptions to guide the users in the identification of their own risk.

2. Ownership of the risk

The Framework contains detailed guidance on the ownership of the risks including Section 6.1 – Governance and Reporting, which notes that risks are captured at divisional and departmental levels on risk registers and will be escalated if they exceed the agreed tolerance level for its category (in line with Section 6.2 Risk Escalation) to the appropriate Tier 2 Risk Registers which are noted as:

- DCC Local Policing
- DCC Crime and Ops Support
- DCO Corporate Management Board
- DCC Designate

Risks that are escalated to Tier 2 Risk Registers are reported to their respective DCC / DCO's management boards where a decision will be taken regarding whether further escalation is required to the Organisational Risk Register, the Audit and Risk Board and the SPA.

In addition, Section 6.3 of the Framework sets out the roles and responsibilities of the following individuals and groups within Police Scotland in respect of risk:

- Chief Constable
- Force Executive
- Audit & Risk Board
- DCC/DCO Tier 2 Boards
- Divisional Commanders / Heads of Department
- Enterprise Risk Manager
- Risk Management Officers
- Risk Owners
- Risk Leads
- Risk Champions

Improvement Opportunities:

- *Within Section 6.2, consider providing further guidance on the decision making process at the DCC/DCO management boards to ascertain whether the risk should be further escalated to the Organisational Risk Register and therefore the Audit and Risk Board and the SPA.*
- *Within Section 6.3, consider including a description of the role / responsibilities of SPA and the SPA Interim Chief Officer (as Accountable Officer) in relation to management of Police Scotland risks.*

Management Response:

- *Management accepts this recommendation. Specific further guidance has now been added to section 6.2 to clarify the process by which risks are further escalated from DCC/DCO management boards to the Organisational Risk Register.*
- *Management accepts this recommendation. A description of the role of both the SPA and SPA Chief Executive have been added to the section at 6.3.*

Action Owner: Enterprise Risk Manager **Due date: Complete**

3. Assessing the risk

Section 7.4 of the Framework includes detailed guidance regarding the assessment and scoring of the risks according to severity. The guidance notes that while risks will be scored at a number of stages during its lifespan, there are two particular scores that must be identified for each risk:

- Untreated score – this represents the gross risk with no controls, mitigation or contingency plans in place.
- Current score – this represents the net risk following consideration of controls, mitigation and contingency plans.

The risk assessment matrix detailed in the Framework is a 5x5 scoring mechanism which will identify a score between 1 and 25. Where risks have more than one category of impact, the highest scoring criteria will identify the overall impact score for that risk.

The Framework also contains a detailed Risk Matrix at Appendix A which lists the risk categories and provides guidance on the scoring criteria to assist users in assessing the scoring of their individual risks.

Improvement Opportunities:

- *Within Section 6.2, consider clarifying whether it is the untreated or current score that is used to determine whether the risk requires to be escalated for further monitoring and oversight.*

Management Response:

- *Management accepts this recommendation. Section 6.2 has been clarified to state that the current score is used to determine risk escalation.*

Action Owner: Enterprise Risk Manager **Due date: Complete**

4. Risk appetite

Police Scotland advised that the section on Risk Appetite within the Draft Risk Management Framework is still under development and, as such, this section has been excluded from our review.

5. Response to risk

There is no guidance within the Framework that directly correlates to this section within the SPFM Risk Management Guidance however Section 7.2 notes “Ongoing management of the risk may well be in conjunction with partner agencies or influence can be exerted over those capable of mitigating the risk to within appetite”.

Improvement Opportunities:

- *Consider updating Section 7.4 to include an example of a risk within the Framework which encompasses the following elements:*
  - *Identification of the risk including cause and impact*
  - *The untreated score determining the likelihood and impact*
  - *The identified controls, mitigation and contingency plans that have been implemented to address the untreated risk*
  - *The current score determining the likelihood and impact.*

Management Response:

- *Management accepts this recommendation. Section 7.4 has been updated to include an illustrative example of a risk which encompasses the above elements.*

Action Owner: Enterprise Risk Manager **Due date: Complete**

6. Reviewing and reporting

The Framework states that the most important part of the risk management process is the ongoing management and review of the risks. There is detailed guidance in the Framework in relation to roles and responsibilities and clear guidelines on the required risk review timescales which are dependent on the current score of the risk as follows:

Very High	**Risk Score 20-25**	Requires monthly monitoring and updates.
High	**Risk Score 12-16**	Requires monthly monitoring and updates.
Medium	**Risk Score 8-10**	Requires quarterly monitoring and updates.
Low	**Risk Score 1-6**	Requires six monthly monitoring and updates.

Appendix 1 – SPFM Principles of Risk Management

1. Identifying the risk

In order to manage risk, an organisation needs to know what risks it faces and to evaluate them. Identifying risks is the first step in building the organisation's risk profile. There is no single right way to record an organisation's risk profile but maintaining a record is critical to effective risk management. The identification of risk can be separated into two distinct phases:

- Initial risk identification – for new organisations, for organisations which have not previously identified its risks in a structured way or for new projects / activities within an organisation; and
- Ongoing risk identification – which is necessary to identify new risks which did not previously arise, changes in existing risks, or risks which did exist ceasing to be relevant to the organisation.

In every case, risks should be prioritised in relation to objectives. Care should be taken to avoid confusion between the impacts that may arise and the risks themselves and to avoid stating risks that do not impact on objectives. Equally, care should be taken to avoid defining risks as simply the converse of the objectives. A statement of a risk should encompass both the possible cause and the impact to the objective which might arise.

2. Ownership of the risk

Risks should be identified at a level where a specific impact can be identified and a specific action or actions to address the risk can be identified. All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed. The risk owner need not be the person who actually takes the actions to address the risk. Risk owners should however ensure that the risk is escalated where necessary to the appropriate level of management.

3. Assessing the risk

It is important to establish a clearly structured process in which both likelihood and impact are considered for each risk and that the assessment of risk is recorded in a way that facilitates monitoring and prioritisation. It will be necessary to develop a framework for assessing risks that evaluates both the likelihood of the risk being realised and the impact if the risk is realised. A categorisation of high / medium / low in respect of each may be sufficient. There is no absolute standard for this – each organisation should reach a judgement on the most productive level of analysis for its circumstances.

Risk assessment should be recorded in a way that demonstrates clearly the key stages of the process. Documenting risk assessment creates a risk profile of the organisation that:

- Facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves);
- Captures the reasons for decisions made about what is and is not tolerable exposure;

- Facilitates recording of the way in which it is decided to address risk;
- Allows all those concerned with risk management to see the overall risk profile and how their areas of particular responsibility fit into it; and
- Facilitates review and monitoring of risks.

Once risks have been assessed, the risk priorities for the organisation will emerge. The less acceptable the exposure in respect of a risk, the higher the priority which should be given to addressing it. The highest priority risks (the key risks) should be given more regular attention at the highest level within the organisation.

4. Risk appetite

The concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk being considered is a threat or an opportunity:

- When considering threats, the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the costs of the exposure should the exposure become a reality and finding an acceptable balance; and
- When considering opportunities, the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

It should be noted that some risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example many organisations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases, organisations need to make contingency plans.

5. Response to risk

Response to risk can be to:

- Tolerate: for unavoidable risks, or those so mild or remote as to make avoidance action disproportionate or unattractive;
- Treat: for risks that can be reduced or eliminated by prevention or other control action;
- Transfer: where another party can take on some or all of the risk more economically or more effectively e.g. sharing risk with a contractor or management techniques such as public / private partnership; or
- Terminate – for intolerable risks but only where it is possible for the organisation to exit.

In choosing between these responses, factors to consider include cost, feasibility, probability and the potential impact. Another factor to consider is the opportunity to exploit the positive impact that might arise whenever tolerating, treating or transferring a risk i.e. where the potential gain seems likely to outweigh the potential downside. It is also important to be aware that excessive caution can be as damaging as unnecessary risk taking.

6. Reviewing and reporting

The management of risk should be reviewed regularly to monitor whether or not the risk profile is changing, to gain assurance that risk management is effective, and to identify when further action is necessary. Procedures should be put in place to review regularly whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks has changed report significant changes which adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process should be reviewed at least once a year to deliver assurance that it remains appropriate and effective.

Key players in the review and reporting processes are Audit Committees and the assurance and advisory work of Internal Audit. However, it is important to note that neither Audit Committees nor Internal Audit can substitute for management ownership of risk or for an embedded review system carried out by the various staff who have executive responsibility for the achievement of organisational objectives.