



# STAFFORDSHIRE POLICE & CRIME COMMISSIONER & CHIEF CONSTABLE OF STAFFORDSHIRE POLICE

## Risk Management Framework and Strategy

**FINAL Internal audit report: 2.18/19**

**9 October 2018**

This report is solely for the use of the persons to whom it is addressed.

To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.



# CONTENTS

1 Executive summary .....	2
2 Detailed findings .....	7
Appendix A: Scope .....	9
For further information contact .....	11

<b>Debrief held</b>	26 September 2018	<b>Internal audit team</b>	Daniel Harris - Head of Internal Audit Angela Ward – Senior Manager
<b>Draft report issued</b>	3 October 2018		
<b>Responses received</b>	5 October 2018 & 9 October 2018		
<b>Final report issued</b>	9 October 2018	<b>Client sponsor</b>	Jane Heppel - Interim Director of Finance John Bloomer - Director of Finance
		<b>Distribution</b>	Jane Heppel, Interim Director of Finance John Bloomer, Director of Finance,

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at <http://www.icaew.com/en/members/regulations-standards-and-guidance>.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Management actions raised for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is solely for the use of the persons to whom it is addressed and for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

# 1 EXECUTIVE SUMMARY

## 1.1 Background

We have undertaken a review of Risk Management as part of the agreed internal audit plan for 2018/19. The focus of the audit has considered the Framework, Methodology and Strategy across both the OPCC and the Force.

Risk management is central to any organisations strategic management and is a fundamental element of good Corporate Governance. It is a means of maximising opportunities and minimising the costs and disruption caused by undesirable events. The mission of the Force is to keep people safe and reassured which can be linked to the risk management processes and structure and ultimately to the Force strategic objectives. Similarly, the OPCC priorities included within the Police & Crime Plan are clearly linked to their Risk Register.

The Office of the Police and Crime Commissioner (OPCC) and Staffordshire Police have two distinct and separate risk registers. Both are bespoke spreadsheets to manage the risk and assurance framework that enables management to monitor and measure overall exposure to risk and examine the effectiveness of controls. The management, reporting and ultimate responsibility of managing these risks contained on the registers falls to risk owners within each of the organisations.

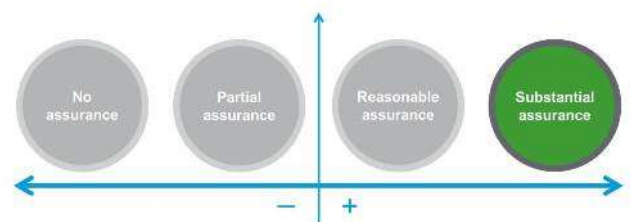
## 1.2 Conclusion

### Force

Our audit confirmed that there is a robust risk management framework in place that provides clarity for risk management, which based on our sample testing we could see is applied across the Organisation. Directorates are very much accountable for risk management across the Force and risks are escalated to the Strategic Risk Register, as and when required.

#### Internal audit opinion:

Taking account of the issues identified, the board can take substantial assurance that the controls upon which the organisation relies to manage the identified area(s) are suitably designed, consistently applied and operating effectively.



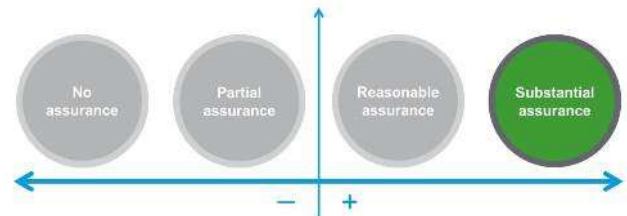
### OPCC

Our audit confirmed that there is a robust risk management framework in place that was clear and was applied consistently across the Organisation, based on our sample testing. Risks are discussed and reviewed at the monthly management team meetings and are managed in accordance with the Risk Management Framework, approach and supporting Policy documentation.

---

**Internal audit opinion:**

Taking account of the issues identified, the board can take substantial assurance that the controls upon which the organisation relies to manage the identified area(s) are suitably designed, consistently applied and operating effectively.



---

## 1.3 Key findings

### Force

#### **Risk, Issue and Opportunities (RIO) Management Procedure**

From review we found that the Risk, Issue and Opportunities (RIO) Management Procedure defines the assessment criteria for risks, issues and opportunities. Additionally, the procedure provides clear guidance on how a risk should be assessed and scored and the requirement to assign a risk lead and owner to every risk. It also defines the Force's Risk Appetite and the links to the governance framework.

#### **Populating Risk Register**

At the time of the audit there were three strategic risks included within the Force Strategic Risk Register. We confirmed that the strategic risks were being reviewed by the Force Strategy Board. As part of the audit we confirmed that for the strategic risks that they had been scored (both inherent and residual) in accordance with the associated policies and procedures.

#### **Force Strategy Board (FSB)**

Each Directorate is required to submit an update of the Strategic Risk Management element to the Force Strategy Board. The summaries are required monthly along with matters by exception that require escalation to the Strategic Risk Register and sample testing confirmed these were being submitted as required. At the Force Strategy Board meeting on 14 June 2018 a risk around data quality was approved for inclusion onto the Strategic Risk Register, following an escalation request from the Directorate. The OPCC attends the FSB to provide an overview of those risks included within the OPCC Risk Register.

#### **Directorate Board**

Oversight, review and accountability happens at Directorate level with the individual Directorate Risk Registers. Risk is a standing agenda item at each Directorate Board. We reviewed the agendas for the Directorate Boards and confirmed that risk was a standing agenda item. It was noted that the Governance Lead attends the Directorate Board, as required, to provide guidance and overview regarding risk management and process.

#### **OPCC and Force**

##### **Training**

Both the OPCC and Force Senior Leaders were invited to attend Risk Management training in January 2018, facilitated by Boeing. We obtained and reviewed the training documentation that was produced for the workshop and confirmed that it was appropriately detailed and reflected the RIO Procedure for the Force and generally reflected the Policy for the OPCC. There are some minor amendments that are required to update the Policy so it is in line with the training delivered, but the OPCC are aware of this and are planning to update as part of the Governance Framework review that is scheduled to take place during quarter 3.

## **Link to Police and Crime Plan Objectives**

From review of the Force and OPCC Strategic Risk Registers (SRR) we confirmed that in all cases the risks had a column completed to denote the area of the Police and Crime Plan and policing objective that the risk is linked to.

## **Risk Scoring Methodology**

From review of both the Force and OPCC Risk Management Policies and Procedures we identified that there was a formal scoring methodology for risks in place which is based upon a 5 x 5 scoring matrix.

From review of the Force's SRR and the OPCC Risk Register we confirmed that all risks are scored via this mechanism both on an inherent and residual basis.

## **Risk Controls & Assurances**

Included within both the OPCC and Force Risk Register are both controls and assurances (using the 3 lines of defence approach) and on review of those assurances it was not clear what the outcome is of those assurances received - whether it be positive or negative and whether any further action is required to address any control deficiencies or negative assurances received. To enhance and improve the purpose of the document it would be beneficial to include any outcomes of the assurances received which will also assist in identifying any gaps in assurance. **(Medium)**

## **Ethics, Transparency, Audit Panel (ETAP) & Finance Panel**

We obtained the ETAP minutes and the Finance Panel meetings from April 2018 and confirmed that there was a record of the Force and OPCC Risk Registers being presented and documented and scrutiny was noted within the minutes.

## **Performance Assurance Board**

We obtained the minutes from the Board from April 2018 and confirmed that Risk was included as an agenda item and it was established that where necessary, i.e where the Force had identified a risk that required escalating to SGB or where a risk had been scored outside of the OPCC risk appetite, the risk had been flagged for consideration and review.

## **Strategic Governance Board (SGB)**

The SGB is the PCC's Strategic Management forum for policing which is attended by the OPCC Senior representation and the Force Chief Officers. On review of the terms of reference we confirmed that Strategic risk reports are included as a set agenda item. On review of a sample of SGB agendas we confirmed that Strategic risk was included. Furthermore, we were able to confirm that where appropriate risks had been escalated to the SGB for review and consideration, recorded and actioned, in accordance with the governance framework. In addition, this forum provides the mechanism for both the OPCC and Force to review and consider both risk registers and highlight any linkages and sense check.

## **OPCC**

### **Populating the OPCC Strategic Risk Register**

We were informed by the Head of Governance and Assurance (OPCC) that the strategic risks were subject to a formal review at each monthly OPCC Management Team meeting where all risks within the SRR are reviewed. This would conclude if the risks were still valid / scored correctly and being mitigated in the correct way. We reviewed the last five monthly meeting minutes and confirmed that the SRR is included as a standing item and from a review of the corresponding minutes we confirmed that clear discussions take place around the risks and their status, together with detailed actions.

## Risk Management Framework and Approach and Risk Management Strategy

The OPCC Risk Management Strategy was devised by the Director of Finance and Performance and was effective as of December 2017. The Strategy informs of the principles to adopt to ensure strategic and operational objectives are met through effective risk management. The Strategy is part of the overarching Risk Management Framework & Approach. Both documents provide clarity and are appropriately detailed to describe the risk management process and roles and responsibilities within the OPCC. It is noted that elements of both the Strategy, Framework and Approach documents refer to incorrect job titles and some of the responsibilities highlighted have changed to alternative officers. However, the Head of Governance and Assurance was aware of the differences and of those elements that require updating and this is part of the overall governance review to be completed later during the year. As this had been identified and action was planned, we have not agreed a formal action within this report.

### Strategic & Operational Risk Register

As part of the audit we reviewed the SRR for June 2018 and confirmed that there were a total of ten strategic risks of which two were outside of the risk appetite, as defined in the OPCC Risk Management and Approach. We confirmed that all strategic risks were being reviewed by the OPCC Management Team. We were also provided with the revised Risk Register template, dated 12 September 2018, which incorporated both operational and strategic risks. As part of the audit we confirmed that for a sample of risks that they had been scored in accordance with the associated policies and procedures.

Generally, the residual risk score depends on whether the risk is to be monitored or managed. As such, mitigating actions are included accordingly. On review of the SRR for June 2018 and the revised version from September 2018 it was clear what the mitigating actions referred to and the intended outcome to assist with the management or monitoring of that risk. Responsible owners had been assigned, together with implementation dates.

We have agreed **one medium** priority management action that is covered within section two of the report

## 1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
OPCC & Force	1	(12)	0	(12)	0	1	0
<b>Total</b>					<b>0</b>	<b>1</b>	<b>0</b>

\* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

## 1.5 Additional feedback

It was pleasing to note that as part of the Risk Management Framework, both the Force and OPCC have a process in place for identifying and recording opportunities. The OPCC record opportunities as part of their action logs from the OPCC Management meetings and the Force record any opportunities as part of the Strategic Risk Register. Horizon scanning is also a standard agenda item at the Performance & Assurance Board meetings. Furthermore, each week the Governance Lead at the Force prepares an Environmental Scan report that is presented to Force Executive each week that details opportunities, particularly around funding opportunities that can be investigated/followed up by the relevant Directorate. The focus on opportunities, although relatively a new concept to the Organisations is certainly good practice and is one that we actively encourage across our client base.

## 2 DETAILED FINDINGS

### Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
<b>Area: OPCC &amp; Force</b>								
1	<u>OPCC</u>  OPCC Operational Risk Registers are in place and since September 2018 they have been incorporated within the OPCC Strategic Risk Register. Controls and assurances are included within the document and are recorded against each risk.	Partly	-	The current format of the Risk Registers for both OPCC and Force sufficiently outline the control frameworks in place for each respective risk and the actions taken to ensure the residual risk is within the risk appetite for each respective category.  Included within the Risk Registers for both the OPCC and Force are both controls and assurances (using the 3 lines of defence approach) and on review of those assurances was not clear what the outcome is of those assurances received - whether	Medium	The assurances that are included within the Risk Register will be expanded further to record the outcome of the assurance that has been received together with any further required actions.	30 September 2018	Head of Governance & Assurance (OPCC) and Governance Lead (Force)



Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management	Implementation date	Responsible owner
	<u>Force</u>  The Strategic Risk Register and Directorate Risk Registers include controls and assurances against each specific risk.			it be positive or negative and whether any further action is required.  To enhance and improve the purpose of the document it would be beneficial to include any outcomes of the assurances received.				

# APPENDIX A: SCOPE

## Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following areas:

### Objectives of the area under review

Adequate and effective processes are in place to identify and manage both risks and opportunities.

### Areas for consideration:

- The Risk Management Strategy / Policy and accompanying procedures and arrangements for regular review and approval;
- Arrangements in place and approach taken to identify the key strategic risks facing the organisations and to keep these risks under review on an ongoing basis. Furthermore, to consider the alignment between different governance groups in respect of risk matters;
- Identified risks are assessed in accordance with an approved risk matrix to provide priority risks for reporting and mitigating action. This will also include 'horizon scanning' and how the organisation ensures that risks are identified sufficiently in advance to allow appropriate action to be taken;
- As well as the identified risks we will consider how opportunities can be identified, ensuring that they link to strategic objectives and how opportunities are assessed in terms of potential outcome and the potential impact of opportunities' missed' or not taken;
- Maintenance, monitoring and updating of Strategic and Operational Risk Registers;
- The processes in place for the escalation of risks including escalation from Operational Risk Registers to Strategic;
- The controls to manage / mitigate risks have been documented and are clear in detail, assigned to nominated persons and a timescale for completion agreed;
- Assurances have been identified (as well as gaps in assurance) and are used to inform the risk management process;
- There is regular reporting of the Risk Register to senior management and the Office of the Police Commissioner and to the Chief Constable. and how this informs decision making. In particular, whether it meets the needs of different levels of management, from operational users through to the Board. We will also include how the reporting mechanism aligns with other performance reporting within the business, i.e. corporate objectives; and

### Limitations to the scope of the audit assignment:

- The scope of the work will be limited to those areas examined and reported upon in the areas for consideration in the context of the objectives set out for this review.
- Any testing undertaken as part of this audit will be compliance based and sample testing only. We will not perform testing to confirm that any mitigating controls that have been identified and recorded on the risk register are actually in place. Similarly, we will not perform any testing to confirm that the sources of assurance that have been identified and recorded are actually in place.
- This review will not comment on whether individual risks are appropriately managed, or whether the organisation has identified all of the risks and opportunities facing it.

- We have not confirmed the attendees of the Risk Management training that was facilitated by Boeing that took place quarter 4 2017/18.
- We will not comment on the scores assigned to individual risks, we will only consider whether a scoring mechanism is in place which is fit for purpose and has been consistently applied.
- We do not endorse a particular means of risk management.

Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

## FOR FURTHER INFORMATION CONTACT

**Daniel Harris - Head of Internal Audit**

[Daniel.Harris@rsmuk.com](mailto:Daniel.Harris@rsmuk.com)

Tel: 07792 948767

**Angela Ward – Senior Manager**

[Angela.Ward@rsmuk.com](mailto:Angela.Ward@rsmuk.com)

Tel: 07966 091471