ITEM 08

PART ONE

To: **Joint Audit Committee**

Date: **18th January 2018**

By: **Alison Bolton, Chief Executive, Office of the PCC**
Helen Bayliss, Head of Service Quality, Surrey Police

Title: **ANNUAL REVIEW OF RISK MANAGEMENT ARRANGEMENTS**

Purpose of report

To present a report on risk management arrangements for Surrey Police and the Office of the Police & Crime Commissioner.

Recommendation

The Committee reviews the arrangements for risk management.

Equality and Human Rights Implications: None arising

Risk: No specific risks arise from this report.

Contact details Alison Bolton, Chief Executive
Telephone number: 01483 630200
Email Address alison.bolton@surrey.pnn.police.uk

Introduction

The Audit Committee is obliged to review the arrangements in place for both Surrey Police and the Surrey PCC in respect of risk management to ensure that they are adequate to effectively manage organisational risk.

Responsibilities for Risk Management

The PCC and the Chief Constable (and their respective senior staff) all ensure that risk is taken seriously by the leaders of the organisations, recognising that significant risks could impede the achievement of the objectives of the Force and/or the PCC. The Audit Committee also reviews risk registers for both organisations and annually reviews the arrangements in place for managing risk.

Office of the PCC (OPCC) Risk Management Arrangements

The PCC's responsibility in terms of risk could be described as three-fold: he must ensure both the Force and OPCC have in place effective risk management arrangements; he must identify and review his own risks; and he must identify and scrutinise the 'high level' risks belonging to the Force or those jointly owned by the Force and PCC.

The PCC's Code of Corporate Governance confirms the PCC's intention to embed risk management within the OPCC and Force by operating a risk management system that aids the achievement of strategic objectives, protects the OPCC and Force's reputation and other assets and is compliant with statutory and regulatory obligations. This system should be capable of formally identifying and managing risks, involve relevant senior officers, map risks to financial and other key internal controls and incorporate business continuity planning. The PCC has committed to reviewing and, if necessary, updating his risk management processes at least annually.

The Office of the PCC's Risks and its Risk Register

The Office of the PCC maintains its own risk register as distinct from the Force. The Chartered Institute of Public Finance and Accountancy (CIPFA) recommends that risk management must clearly focus on those significant risks that would prevent the organisation achieving its key business objectives. It suggests that the number of significant business risks to which senior management attention should be drawn is no more than 10 to 20. The Office of the PCC has worked on this basis with its risk

register. The PCC's register uses weightings to assess risk, sorting risk by impact and probability.

The PCC's risk register is brought to every meeting of the Audit Committee. The Audit Committee reviews the risk register to examine risk scores and control measures and assess whether it recommends that any risks can be closed or should be added to the register. The Committee's Terms of Reference reflect this responsibility. The OPCC Secretariat reviews the register on at least a monthly basis at its team meetings and makes recommendations for changes to ratings to the PCC.

The PCC's Assurance Framework and Business Continuity Plans

The OPCC maintains an assurance framework which has been developed to identify the internal controls in place to ensure that the OPCC discharges its accountabilities – and in particular its statutory responsibilities - properly. Whilst the risk register comprises only those more critical risks that can be anticipated and dealt with, the assurance framework covers other eventualities. The framework is reported regularly to the Audit Committee.

The PCC has drawn up comprehensive business continuity plans. These are tested regularly by the OPCC Secretariat.

Decision-making

To help the OPCC in making decisions and managing its business, all reports submitted by the Chief Constable to the PCC's oversight meetings include an assessment of risk and how the risks will be mitigated. The PCC applies this same principle when considering papers for his own 'key decisions'.

Jointly Owned Risks – PCC and Surrey Police

Some risks are likely to impact on both the Force and the PCC and as such, are deemed jointly owned risks. Jointly owned risks are considered at meetings of the Strategic Risk and Learning Group (SRALG), chaired by the Deputy Chief Constable and to which the Chief Executive of the OPCC attends. They are also reported to the Audit Committee, which allows the PCC further oversight.

The Force and OPCC also recognise that, on occasions, a risk may have different impacts on either organisation. This can result in the same issue being differently classified or mitigated by either organisation.

PCC Oversight of Surrey Police Risks

The Chief Constable brings a report on risks by exception, or all high risks and joint risks to every meeting of the Audit Committee, which also enables the PCC to have oversight.

The Authority's Chief Executive receives updates after every SRALG and Strategic Change Board which oversees significant change programmes in hand and routinely monitors project and programme risks.

Surrey Police Risk Management

A management structure and process, supported by appropriate technology, has been implemented to enable:

- Identification of internal and external organisational risks.
- Formal initial and periodic evaluation of organisational risks, using a standard corporate methodology.
- Development of appropriate control strategies and on-going monitoring of progress and impact.

The process covers the identification, measurement and recording of organisational risk for both the Force and the PCC, the definition and monitoring of control measures to reduce or negate the risk (or the decision to tolerate it if no control measures are appropriate), and the on-going appraisal of the impact of control measures on the scale of the risk.

Chief Officers and senior managers identify risks relating to their portfolio of responsibility at their respective management meetings. These are held monthly and are attended by senior staff members from the within their business area.

Senior management teams will also consider potential risks and decide whether an actual risk is posed and what evidence exists to corroborate the risk. In the first instance, the management meeting will decide whether an identified risk is considered as suitable for their management or portfolio management.

Risks are scored against a matrix that assesses both the probability and the impact of the risk. The portfolio/business lead also decides whether the risk is a 'Force level risk' or a 'Portfolio level risk' - Level 1 Assessment. See appendix 1.

To aid consistency the Force's level of tolerance towards risk across the different impact areas (i.e. the 'risk appetite') has been agreed, and is outlined in the 'Risk Tolerance Framework'.

Once the risk has been identified and assessed a risk or an issue an appropriate response or control strategy is devised.

All details (including the categorisation of risk, risk description, risk events, risk assessment, control strategy and control measures) are recorded on to the Risk Management Database (Risk Register).

Determining a critical risk can be subjective but with the correct application of the risk matrix the risk score will provide an effective basis on which to decide whether the risk should go to the Chief Officer Group.

This will be determined by the Deputy Chief Constable at SRALG who monitor all organisational risks. The Chief Officer Group (COG) will then decide whether to manage Force risks coming to their attention or monitor SMT/Portfolio management.

Subsequent meetings review existing risks, progress of control measures and re-assess the risk scoring and control measures as appropriate. This takes place monthly at SMT and bi-monthly at SRALG meetings .The progress and impact of control strategies will be examined and any adjustments necessary made.

The Joint Audit Committee will regularly review the Risk Registers and Assurance Frameworks for both the PCC and the Force and provide assurance that risk management arrangements are adequate.

Risks categorised as 'Portfolio/Business level risks may be closed at a management meeting by the Portfolio/business lead – once it is agreed that the risk no longer applies.

Critical risks may only be closed by SRALG.

- **Everyone** - within the organisation has a responsibility to identify risk and report it to their line manager for a decision as to whether it should be forwarded to their SMT for management
- **The Chief Constable and the Police and Crime Commissioner (through his Chief Executive and Chief Finance Officer)** - are jointly responsible for the management of risk through an agreed strategy and process. The PCC has responsibility for maintaining a strategic oversight of its own and the Force's risks and the risk management process.
- **Portfolio Owners** (Chief Officers) - have responsibility for identifying, owning and managing risk relating to their portfolio of responsibility or organisational risks that are within their capacity to manage through their respective monthly SMT's.
- **SMT Members -** senior staff members from the within the portfolio, feed in risks from their own units and strands and undertake responsibility for any risk control measures assigned to them.
- **Business Leads -** have responsibility for identifying and managing risks that are relevant to their area of business and are within their capacity to manage.
- **Strategic Risk and Learning Group** has responsibility to monitor, escalate and close risks**.**
- **COG -** has responsibility for managing Force critical risks and monitoring risks escalated to them by the DCC.
- **Service Quality Manager -** will be the Risk Manager for the Force and responsible for reviewing and updating risk strategy, policy, risk management process and administering the database. Act as an advisor on risk to Senior Officers and Business Leads and independently review risk management and control strategies.

Audit and Inspection of Risk Management Arrangements during 2017

The Internal Audit function contracted by the PCC reviews areas identified on the risk register of the Force and the PCC on a regular basis as part of the Internal Audit Plan. Findings are reported to the Audit Committee.

The internal auditors undertook an audit of the PCC and Force risk management framework in June 2016. The audit evaluated the effectiveness of the risk management arrangements by reviewing the processes for the identification, ongoing monitoring and management of key risks. The recommendations (none of which were graded 'high') from this audit have been reported to the Audit Committee. The internal audit opinion stated that the Force and OPCC can take reasonable assurance that the controls upon which the organisation relies to manage this area are suitably designed and consistently applied.

Appendix 1

Risk Tolerance Framework	
Low Tolerance:	
Impact Area	**Comment**
Financial	Funding gap/ Duty of prudence with public funds
Reputation	Public support is crucial
Legal Compliance	We must uphold the law
Staff safety	
Public Safety	The aim of Surrey Public First
Medium Tolerance:	
Impact Area	**Comment**
Performance	We will set minimum acceptable levels
High Tolerance:	
Impact Area	**Comment**
Home Office/ACPO Compliance	We will act in the best interests of the Force and the public of Surrey.

PROBABILITY Assessment		**Impact Time-scale**	
Almost certainly will not happen	**1**		
Very unlikely to happen	**2**	**How soon will the impact be felt:**	
Quite possibly will happen	**3**	6 months	**Short term**
Probably will happen	**4**	6 – 18 months	**Medium term**
Certain to happen	**5**	More than 18 months	**Long term**

IMPACT Assessment (the consequences if this risk happens)					
Impact Grading	**Impact Categories**				
	Safety	**Reputation**	**Performance**	**Compliance**	**Financial**
1. Negligible	No injury	No discernable damage	No discernable impact on achieving performance targets	No breach of policy & procedure	On or within allocated budget
2. Only a small effect	Minor injury	Minimal localised damage	Minimal impact on achieving performance targets	Non-compliance with policy & procedure	Within agreed tolerance
3. Noticeable effect	Serious injury	Limited short-term damage	Relevant & noticeable impact on achieving performance targets	Non-compliance with regulatory framework	Additional funds required

4. Serious problem with significant impact	Single fatality / long-term impact on quality of lives	Major long-term damage	Major impact on achieving performance targets	Improvement notice / civil litigation	Significant impact on other budget(s)
5. Critical Issue that will have considerable impact on the organisation	Multiple fatalities / long-term impact on quality of lives	Catastrophic damage	Catastrophic impact on achieving performance targets	Criminal prosecution / serious intervention	Potential loss of other budget allocations

RISK MATRIX

Probability		1	2	3	4	5
5	5	Low 5	Medium 10	Medium 20	VERY HIGH 40	VERY HIGH 80
4	4	Low 4	Low 8	Medium 16	HIGH 32	VERY HIGH 64
3	3	Low 3	Low 6	Medium 12	HIGH 24	VERY HIGH 48
2	2	Low 2	Low 4	Low 8	Medium 16	HIGH 32
1	1	Low 1	Low 2	Low 4	Low 8	Medium 16
		1	2	4	8	16

Impact

RISK SCORE	
>= 40	VERY HIGH
> 20	HIGH
>= 10 <= 20	Medium
<10	Low