THE POLICE AND CRIME COMMISSIONER FOR NORTH YORKSHIRE AND THE CHIEF CONSTABLE FOR NORTH YORKSHIRE POLICE

Risk Maturity

FINAL

Internal Audit Report: 1.15/16

17 February 2016

CONTENTS

Debrief held	13 January 2016	**Internal Audit team**	Dan Harris, Head of Internal Audit Angela Ward, Senior Manager Lindsay-anne Straughton, Client Manager Anastasia Morgan, Senior Auditor
Draft report issued	22 January 2016		
Responses received	17 February 2016		
Final report issued	17 February 2016	**Client sponsor**	Tim Madgewick, Chief Constable Joanna Carter, Chief Executive Officer
		Distribution	Tim Madgewick, Chief Constable Joanna Carter, Chief Executive Officer Donald Stone, Risk and Assurance Manager

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. Recommendations 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. Therefore, the most that the internal audit service can provide is reasonable assurance that there are no major weaknesses in the risk management, governance and control processes reviewed within this assignment. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. 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 party other than the Board which obtains access to this report or a copy and chooses to rely on this report (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 our Client 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.

1 EXECUTIVE SUMMARY

1.1 Background

We have undertaken a review of Risk Maturity, where we have examined the current processes and systems for the identification, recording, assessment, controls/ mitigations, assurance, monitoring and reporting of risk with the Police and Crime Commissioner (PCC) for North Yorkshire and the Chief Constable (CC) for North Yorkshire.

The review included assessing the process to manage the following risks identified by Internal Audit:

- The organisations do not adequately identify and/or manage risks to delivery of the Police and Crime Plan.
- The organisations do not identify and appropriately respond to opportunities.

The PCC and the CC utilise the Active Risk Manager (ARM) system to document risks, both operational and strategic. ARM was also used to log project risks across the organisations and risks which had arisen from HMIC and Internal Audit reports.

The Risk and Assurance Team is responsible for oversight of ARM and risks, however they are not responsible for the management of risks. The Risk and Assurance Team, led by the Risk and Assurance Manager coordinates risk management processes across the organisations.

1.2 Conclusion

We reviewed the design and application of the control frameworks and have agreed with management, actions where these can be improved in line with good practice.

Through discussion with staff and review of documentation it is our opinion that risk management across the organisations was well embedded; Strategic risk owners gave good feedback in regards to how risk management has developed and that the risk register was now a ‘live’ document used for planning and prioritisation of day to day tasks.

It was noted that the organisations assess risks using a 4 by 4 risk matrix, assessing the likelihood of the risk materialising and the impact. Current risk scores take into account controls currently present and actions are then identified by the organisation to reduce the risk to the organisations appetite level; an element which is often missing at other clients in the sector.

Although there were minor areas for improvement, overall risk management was well embedded within organisation processes and procedures. Discussion with the Risk and Assurance Manager and the Risk Manager and Service Review Manager and review of the staff intranet for Risk and Assurance, identified that the Risk Policy and associated documentation were on the intranet and available for all staff.

Along with the Policy, there was a Risk Appetite document, Risk Management Strategy and Risk Identification Template. Review of all the documentation confirmed that the risk management process was adequately documented.

Discussion with the Risk Assurance Manager established that on a quarterly basis Risk Champion Workshops were held which included all Risk Champions across the organisation and the Risk Assurance Team. During the meeting ideas are shared on supporting business areas with the risk management process and updates provided in relation to ARM.

Review of all 12 red strategic risks and 10 operational risks across five departments (Information Management, HR, Estates, Corporate Communications and Major Crime), confirmed that in all cases the causes and consequences of the risk were detailed on ARM. Furthermore, all risks were related to a strategic objective (priority) detailed within the Police and Crime Plan and scored using the scoring matrix

The Strategic Risk Register is presented at the Joint Corporate Risk Group on a monthly basis to review and challenge risks. Review of the monthly meeting minutes from April 2015 to October 2015 identified that the strategic risks from ARM were reviewed, which included risks to be escalated and removed and trigger dates (risks in proximity).

The Corporate Performance, Scrutiny and Delivery Group receive reports from the Joint Corporate Risk Group on significant matters and key emerging themes and associated management activity. Review of the agenda for November 2015 and October 2015 confirmed the report was discussed.

Review of recommendations from previous Risk Reviews performed by Internal Audit established that two recommendations had been raised and recorded on ARM. One, that the Risk Management Policy should provide clarity on escalation of risks to strategic level, and one in regards to the Risk and Assurance Unit in promoting the periodic completion of SWOT analysis or similar assessments across the organisation. Testing performed as part of this review confirmed that both of these had been addressed.

It was also noted that previous actions identified during Internal Audits and HMIC inspections were added to ARM on a one to one relation, leading to large numbers of risks and actions. However, these are becoming more streamlined and actions are now collated against the most appropriate risk(s).

We have assessed the organisations risk management framework and confirmed that the status of the organisation in relation to Risk Maturity can be described as **“Developing”** to **“Mature”** on the RSM Risk Maturity Scale. This conclusion was formed by undertaking interviews with key employees and conducting analysis of both Strategic and Operational Risk Registers.

	Increasing risk maturity →			
	Emerging	Developing	Maturing	Enabling
	Informal approach to risk management	Risk management approach adopted to meet basic expectations of stakeholders	Risk management approach built into normal business process	Risk management supports the delivery of strategic objectives
Governance	Risk management only considered at certain levels of the business	A defined risk management approach and risk is captured at all levels of the business	An established risk management approach with clear linkages between each risk level	Risk management directly informs business planning and supports business decisions
Risk identification	Ad hoc risk identification	Annual risk assessment	Continuous risk identification undertaken with clearly defined risks using cause and effect analysis	Risk identification embedded in the activities of the organisation for all operations
Risk assessment	Basic risk assessments using impact and likelihood	Identification of a risk scoring matrix with clearly defined definitions for impact and likelihood	Consistently applied risk scoring methodology assessing risk both inherently and residually	Management challenge and consider risk appetite for each risk type
Risk mitigation	Mitigations identified that manage risk	Mitigations are specifically separated between existing controls and identified actions	Efficient and effective mitigations established	Mitigations are achieving the required outcomes
Assurance	Assurance mechanisms in place	Assurances mechanisms are defined and reported on	Direct linkage between assurances and mitigations	Assurance outcomes are used to drive to inform the Organizational risk profile
Monitoring and reporting	Informal communication of risk	Cyclical risk management reporting	Risk management 'check and challenge' at all levels of the business	Risk management used to optimize decision making

The main areas for improvement where management actions have been agreed were as follows:

- Review of a sample of 12 red strategic risks identified that in one case current controls had been documented however in the remaining 11 risks controls had not been identified. For the one risk where controls were detailed, we found that the controls were not controls but were future actions or 'statements' with insufficient detail.

  For a sample of 10 operational risks we found that no current controls were documented.

- For two of the 12 strategic risks it was found that actions had passed their response due by date but no response had been provided on ARM, nor had a review of the risk been undertaken to provide an update on the action.

  For a sample of 10 operational risks we identified in one case the response due date for an action had passed and in three cases no response due date was entered onto ARM.
- For two of the sampled 12 red strategic risks it was identified that all actions had been implemented, however the current risk score had not reached the residual risk.

  A report was obtained which identified eight strategic risks where the current risk score had not changed since the risk had been added. In three cases the risk actions were either complete or over 50% of the actions had been implemented, but the current risk score had not been updated.
- We identified nine strategic risks and five operational risks where the risk rating was at the residual rating, yet further actions had been identified and in some instances still being implemented. In addition, further review of 12 strategic risks established that in six cases the actions detailed did not reduce the impact of the risk if it materialised, only the probability of the risk materialising.
- We highlighted that the organisations had not identified within the risk registers how they gain assurance that mitigating controls are in place and working effectively. Assurances were however provided to the organisations via the Future External and Internal Inspection Activity report presented to the JCRG, these had just not been linked back to specific risks and/or strategic priorities.

Further details can be found in section 3 of this report.

1.3 Additional feedback

We have also identified innovation or good practice at similar organisations in relation to opportunity management that the you may wish to consider:

Good practice for further consideration

Horizon scanning was performed by Operational Policing at North Yorkshire, and by West Yorkshire Police which is then shared with North Yorkshire. However, it was not currently performed for North Yorkshire at a corporate level. Management have identified that this was in development for the next financial year and draft documents were reviewed to confirm that this was in progress therefore no formal management action has been raised.

When deliverables are identified in order to meet the Strategic Priorities of the Police and Crime Plan, current strategic risks are aligned with deliverables. In future with horizon scanning, risks will be identified that may affect the organisation meeting its Strategic Priorities within the Police and Crime Plan. These risks identified during horizon scanning may be risks which could be seen to be an opportunity which the organisation may wish to explore.

Three key areas we are increasingly finding that organisations are looking at are:

1. Performance

Examples:

- Organisations create opportunities by evaluating current partner relationships, and creating new relationships with partners that create innovation and security.
- Evaluate major industry trends and leverage insights from successful competitors and market entrants.

2. Embedding Risk Management processes

Examples

- Identify and design areas that can improve core processes and sub-processes.
- Undertake enterprise risk assessment to identify, assess and rank key business risks and opportunities across the business.
- Communicate risk tolerance across the organisation including their board, senior management, and staff.

3. Identifying IT and information security risks and opportunities

Examples

- Evaluate existing IT costs and systems for opportunities to improve efficiency.
- Include information security in all initiatives to reduce costs.
- Reduce the cost of information security and try to eliminate duplication using a zero-based security approach.
- Develop a system to identify and prioritise security risks and monitor spending on IT to ensure costs are within definite boundaries.

North Yorkshire may also want to exploit the opportunity that a risk presents and provided this is managed well, this should be encouraged. In order to effectively identify opportunities, North Yorkshire should have clear risk appetite limits in place; risk appetite is assessed on a risk by risk basis at North Yorkshire, therefore opportunity management should be built into horizon scanning going forward in order to ensure it is embedded.

2 ACTION PLAN

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 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, with a high degree of certainty, lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The table below sets out the actions agreed by management to address the findings:

Ref	Findings summary	Actions for management	Implementation date	Responsible owner
Risk 1: The organisation does not adequately identify and/or manage risks to delivery of the Police and Crime Plan.				
1	Review of a sample of 12 red strategic risks identified that in 11 instances risks controls had not been identified. For the one risk where controls were detailed, we found that the controls were not controls but were future actions or 'statements' with insufficient detail. For a sample of 10 operational risks it was found that no current controls were documented.	Key existing controls identified for new risks presented at the JCRG will be documented on ARM along with activities to reduce likelihood and impact.	30 June 2016	Donald Stone, Risk and Assurance Manager

Ref	Findings summary	Actions for management	Implementation date	Responsible owner
2	For two of the 12 strategic risks we found that actions had passed their response due by date but no response had been provided on ARM, nor had a review of the risk been undertaken to provide an update on the action. For a sample of 10 operational risks we identified in one case the response due date for an action had passed and in three cases no response due date was entered onto ARM.	Gap analysis or trends of non-compliance will be reported to JCRG on an exception basis. These will feature as part of the regular Strategic Risk Register report.	30 April 2016	Donald Stone, Risk and Assurance Manager
3	For two of the sampled 12 red strategic risks we identified that all actions had been implemented, however the current risk score had not reached the residual risk. A report was obtained which identified eight strategic risks where the current risk score had not changed since the risk had been added. In three cases the risk actions were either complete or over 50% of the actions had been implemented, but the current risk score had not been updated.	When actions are implemented, a review will take place to assess whether the implemented actions have affected the current risk as intended. If so, the current risk rating will be reduced. If the action has not reduced the current risk rating as intended, further actions will be identified and documented or risk tolerance rationale recorded.	30 April 2016	Donald Stone, Risk and Assurance Manager
4	Review of the 12 strategic risks established that in six cases the actions detailed did not reduce the impact of the risk if it materialised, only the probability of the risk materialising.	Where the current risk rating is assessed as matching the residual risk rating, an assessment will be made by the organisation as to whether the risk can be tolerated.	30 April 2016	Donald Stone, Risk and Assurance Manager
5	It was highlighted that the organisation had not identified within the risk registers how it gains assurance that mitigating controls are in place and working effectively.	Sources of assurance identified on the Future External and Internal Inspection Activity schedule will be linked to the	30 June 2016	Donald Stone, Risk and Assurance Manager Lesley

Ref	Findings summary	Actions for management	Implementation date	Responsible owner
		organisation strategic priorities to identify whether appropriate assurance is in place across the organisation. This may be done as part of the business planning process.		Whitehouse, Risk & Assurance Manager

3 DETAILED FINDINGS

3.1 Governance

3.1.1 Risk Management Policy and Associated Documents

Discussion with the Risk and Assurance Manager and the Risk Manager and Service Review Manager, and review of the staff intranet for Risk Assurance identified that the Risk Policy and associated documentation were on the intranet available for all staff.

Review of the Risk Management Policy established that it detailed the risk management roles and responsibilities of groups and individuals across the organisation.

Review of the Risk Appetite document established that it detailed the definition of a strategic risk, the risk appetite and the frequency of monitoring dependent on the category of the current risk. It also detailed the strategic risk escalation process from operational registers.

It was deemed that the content provided in the documents sufficiently detailed guidance for scoring risks and provided adequate guidance to employees on the risk process that should be followed.

Review of the Risk Identification Template identified that it detailed the definition for current controls, current (pre management scores), residual / target (post management scores) and responses required to address the risk.

3.2 Risk Identification

3.2.1 Identifying Risks

In a risk mature organisation risks are captured via two mechanisms, a ‘bottom up’ approach and a ‘top down’ approach. The ‘top down’ approach is driven by the Senior Management and high level strategic risk should be derived from strategic objectives and key business drivers. This is extremely useful when strategic direction is a key factor.

Discussions with the Risk and Assurance Manager established that during monthly Joint Corporate Risk Groups (JCRG), emerging risks are identified and added to ARM via a ‘top down approach’. Review of the monthly JCRG meeting minutes from April 2015 to October 2015 identified that the strategic risks from ARM were reviewed. It was established that one emerging risk had been identified by the group in October in relation to Emergency Services Mobile Communications ~~Plan~~ Programme (ESMCP).

Risks feed upwards via a ‘bottom up’ approach through operational risks within the ARM systems, which may then be escalated to strategic risks.

Operational risks were identified through internal audit, external audit, Risk Assurance Unit audits and other external inspections and these were presented to the JCRG and discussed to confirm the ratings, mitigations and actions identified.

Discussion with the Risk Manager and Service Review Manager established that the exiting practice is to record risks and actions identified through HMIC or Internal Audit in the relevant Business Area risk register or make necessary adjustment or reference if they were already recorded on ARM.

3.2.2 Capturing Risks

Once risks have been identified it is essential that they are captured and recorded on the risk register using clear and concise language. This ensures that when risks are reviewed and scrutinised time is spent reviewing the risks and not re-writing or trying to understand overcomplicated and technical language.

Discussions with the Risk and Assurance Manager established that the Risk and Assurance Team have oversight of the Strategic Risk Register.

Across the Organisation Risk Champions were in place to assist and support departments in regards to identifying and recording risks onto ARM.

Review of all 12 red strategic risks confirmed that in all cases the causes and consequences of the risk were detailed on ARM. Furthermore, all risks were related to a strategic objective detailed within the Police and Crime Plan.

Review of a sample of 10 operational risks identified across five departments; Information Management, HR, Estates, Corporate Communications and Major Crime, in all cases it was confirmed that the causes and effect of the risks had been documented and the risks had been linked to a strategic priority.

3.3 Risk Assessment

3.3.1 Risk Matrix Scoring System

Review of the Risk Management Appetite document confirmed there was adequate guidance in place relating to scoring the risk.

Review of the scoring matrix identified that the impact of the risk was broken down into:

- Financial;
- Reputation;
- Operational; and
- Legal and Compliance

Each of the four elements had the score of negligible, minor, significant and severe. A description of each was detailed. The probability was categorised as highly probable, probable, unlikely and highly improbable.

For all red strategic risks and for a sample of 10 operational risks it was confirmed that the scoring matrix had been applied consistently.

3.4 Risk Mitigation

The risk rating is the current risk category (an as at today professional judgement) taking into account existing controls. . The residual category recorded in ARM is the level of risk after all mitigating controls have been applied.

Review of a sample of 12 red strategic risks identified that in one case current controls had been documented however; in the remaining 11 risks controls had not been identified.

For the one risk where controls were detailed, it was found that the controls were not controls: in one case the control was a future action and the remaining control was a statement with insufficient detail.

For a sample of 10 operational risks it was found that no current controls were documented.

Discussion with Strategic Risk Owners identified that controls were in place for risks, these were just not always documented on ARM. When new risks arising from internal audit, external audit, Risk Assurance Unit audits and other external inspections are presented to JCRG, the mitigations (controls) are discussed however, without recording these mitigations on ARM the process by which risks are added, discussed and rated may not always be transparent.

Management Action
Key mitigations identified for new risks presented at the JCRG will be documented on ARM.

3.5 Risk Appetite and Further Actions

3.5.1 Further Actions

We confirmed that where the current risk rating was above the residual risk rating, actions were identified to reduce the current risk to the residual risk, which were documented with an action owner and a response due by date.

3.5.2 Actions documented on ARM

For a sample of 12 red strategic risks and 10 operational risks it was established that in all cases actions had been detailed.

- For two of the 12 strategic risks it was found in two cases that actions had passed their response due by date but no response had been provided on ARM, nor had a review of the risk been undertaken to provide an update on the action.
- For two of the 12 red strategic risks it was identified that all actions had been implemented, however the current risk score had not reached the residual rating.
- For a sample of 10 operational risks it was identified that in two cases, no actions had been documented as in both cases the current risk and residual were the same and the risk had been documented in order to monitor the risk.

However, in one case the response due date for an action had passed and in three cases it was found that no response due date was entered onto ARM in relation to the actions.

Management Action
Gap analysis or trends of non-compliance will be reported to JCRG on an exception basis.

3.5.3 Action Effectiveness

As per the Risk Identification Template, once responses, including actions, have been identified, the residual target score should be re-calculated to reduce the probability and or impact of the risk materialising.

It was stated that when risk owners updated or closed actions that they should assess the impact of the action in place, in order to identify whether the current risk score had changed.

For two of the sampled 12 red strategic risks it was identified that all actions had been implemented, however the current risk score had not reached the residual risk. The organisation had not reviewed these risks where all the actions had been implemented in order to decide whether further actions were required to reduce the current risk to the residual risk, or whether the risk could be tolerated at its current level.

A report was obtained from ARM, which identified eight strategic risks where the current risk score had not changed since the risk had been added. In three cases the risk actions were either complete or over 50% of the actions had been implemented, but the current risk score had not been updated.

Review of 10 operational risks identified that in all cases the current risk score had not moved since the risk had been identified however, in one case no actions were required as the current risk was at the residual risk score, for nine risks, actions were in progress or not yet implemented therefore the risk rating had not yet been re-assessed, and in one case there were no actions, with the current risk amber and the residual green.

Without reviewing the current risk score when actions have been implemented there is an increased risk that the current risk score may not be up to date and accurate which does not provide management with a clear oversight of the risks, which could lead to inappropriate decision making.

Furthermore, actions may be required to mitigate the risk to the residual risk score required which are not identified.

Management Action
When actions are implemented, a review will take place to assess whether the implemented actions have affected the current risk as intended. If so, the current risk rating will be reduced. If the action has not reduced the current risk rating as intended, further actions will be identified and documented.

3.5.4 Action Efficiency

Actions ware detailed in order to mitigate the current risk's probability and impact to within the organisations risk appetite. Review of all 29 strategic risks identified that nine risks had the same current and residual risk score, however further planned actions had still been identified.

For 10 operational risks sampled it was identified in five cases that the current risk and the residual risk were the same, however in four cases actions had been identified which were in progress of being implemented.

In addition, further review of 12 strategic risks established that in six cases the actions detailed did not reduce the impact of the risk if it materialised, only the probability of the risk materialising.

If mitigating actions do not reduce the current risks, or additional mitigating actions are put in place where the risk already sits within the organisations risk appetite for tolerance, resource and time could be wasted implementing and maintaining actions which are not required.

Management Action
Where the current risk rating is in line with the residual risk rating, an assessment will be made by the organisation whether the risk can be tolerated.

3.6 Sources of Assurance

Sources of assurance can be used to provide assurance to the JCRG and Audit Committee that the controls which mitigate the risks actually exist and are operating effectively.

It was highlighted that the organisation had not identified within the risk register how it gains assurance that mitigating controls are in place and working effectively.

However, the organisation had documented assurances via the Future External and Internal Inspection Activity 2015/16 schedule which was presented to the JCRG, these had just not been linked back to the risks and strategic priorities to enable the organisation to assess whether there were duplications or gaps and how effective the sources of assurance were.

Without assessing the level of assurance received in relation to mitigating controls and management of risks for strategic priorities, the organisation may be relying on a source of assurance to help mitigate against a high risk when in reality it only provides a low level of assurance or the organisation may have over assurance on one priority against another priorities which has little assurance

Management Action
Sources of assurance identified on the Future External and Internal Inspection Activity schedule will be linked to the organisation strategic priorities to identify whether appropriate assurance is in place across the organisation. This may be done as part of the business planning process.

3.7 Monitoring and Reporting

3.7.1 Joint Corporate Risk Group

Review of the monthly meeting minutes from April 2015 to October 2015 identified that the strategic risks from ARM were reviewed.

In all cases the Strategic Risk Register was presented, along with appendices detailing risks to be escalated and de-centralised and trigger dates.

3.7.2 Corporate Performance, Scrutiny and Delivery group (CPSDB)

Review of the Monthly Report of Strategic Risks highlighted by Joint Corporate Risk Group brief for CPSDB confirmed that the report was to bring to the attention of the CPSDB members. The report was to view the potential impact of the risks and whether the members were experiencing ongoing issues or are being impacted by external factors which members may wish to take a view on/ or instigate wider support action/mitigation.

Review of the report identified that it detailed the new risks which had been added or escalated to the Strategic Risk Register.

Review of the report for the 23rd November 2015 and 27th October 2015 confirmed that they were detailed.

APPENDIX A: SCOPE

Scope of the review

The Internal Audit assignment has been scoped to provide assurance on how the Police and Crime Commissioner for North Yorkshire and North Yorkshire Police manages the following area(s).

Objective of the area under review	Risks relevant to the scope of the review	Risk source
Adequate and effective processes are in place to identify and manage both risks and opportunities.	The organisation does not adequately identify and/or manage risks to delivery of the Police and Crime Plan. The organisation does not identify and appropriately respond to opportunities.	Internal Audit

3.3 Scope of the review

We have undertaken a Risk Maturity review, using our in-house developed assessment tool.

We have also taken into account the findings from risk management reviews undertaken by the previous Internal Auditors, and considered how well these had been addressed and embedded.

Our review considered the risk management arrangements at the Police and Crime Commissioner for North Yorkshire and North Yorkshire Police in the following areas:

Governance – the processes in place to define and capture the risk appetite of the organisation, in particular, the linking of appetite to corporate objectives, identification and distinction between strategic and operational risks, and roles and responsibilities of risk owners. We have also considered how the organisation ensures that there is alignment between different governance groups in respect of risk matters, for example between the Joint Corporate Risk Group and the Performance Group.

Risk identification – the avenues in which risks were identified and the frequency of identification, whether there was an assessment of cause and effect for risks, whether risks were linked to strategic objectives, and whether risk and identification was embedded within organisation's operational activities. This has also included 'horizon scanning' and how the organisation ensures that risks were identified sufficiently in advance to allow appropriate action to be taken.

Risk assessment – a review of how risks were scored, whether there were clearly defined definitions for impact and likelihood, and whether scoring methodology was consistently applied.

Risk mitigation – a review of existing mitigations and actions, whether these were efficient and effective and whether these were likely to achieve the required outcomes.

Assurance – whether there were assurance mechanisms in place which were linked to mitigations and were reported upon to relevant recipients at the appropriate frequency.

Monitoring and reporting – the frequency and level of risk reporting 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. This has also included how the reporting mechanism aligns with other performance reporting within the business, i.e. corporate objectives.

Opportunities - we understand that the identification and management of opportunities is an area which the Police and Crime Commissioner for North Yorkshire and North Yorkshire Police wish to develop, and therefore as part of this review we have provided guidance as to how can be achieved through the existing risk management framework. This has included:

- How opportunities can be identified, ensuring that they link to strategic objectives.
- How the organisation can assess both the potential outcome of opportunities taken and the potential impact of opportunities' missed' or not taken.
- How opportunities can be used to feed into the organisations planning processes.

The following limitations apply to the scope of our work:

- This review has not confirmed that the Police and Crime Commissioner for North Yorkshire and North Yorkshire Police have identified all of the risks and opportunities facing it.
- We have not commented on the scores assigned to individual risks, we have only considered whether a scoring mechanism was in place which is fit for purpose and had been consistently applied.
- We have not performed testing to confirm that mitigating controls identified and recorded on the risk registers were actually in place.
- We have not performed testing to confirm that sources of assurance identified and recorded were actually in place.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Please note that the full scope of the audit can only be completed within the audit budget if all the requested information is made available at the start of the audit, and the necessary key staff are available to assist the audit process during the audit. If the requested information and staff are not available we may have to reduce the scope of our work and/or increase the audit budget. If this is necessary we will agree this with the client sponsor during the audit.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit

- Donald Stone, Risk Assurance Manager
- Lesley Whitehouse, Risk Manager and Service Review Manager
- Joanna Whyte, Service Review Manager
- Judith Nellist, Business Planning and Support Manager
- Sarah Wintringham, Head of Information Management
- Maria Earles, Head of Organisational Development
- Richard Flint, Head of Estates, Logistics and Technology
- Chief Superintendent Amanda Oliver
- Hilary Day, Project Manager, Organisational Development

Documentation reviewed during the audit:

- Risk Management Policy
- Risk Appetite
- Risk Strategy
- Risk Identification Template
- Joint Corporate Risk Group Meeting Minutes
- Corporate Performance, Scrutiny and Delivery Group Meeting Minutes
- Active Risk Manager

APPENDIX C: RISK MATRIX AND SCORE

Risk Matrix

Probability	**Nil**	**Highly Improbable**	**Unlikely**	**Probable**	**Highly Probable**
Probability of occurring	Nil	Less than 20%	Between 20 and 40%	Between 40 and 60%	Greater than 60%
Impact	**Nil**	**Negligible**	**Minor**	**Significant**	**Severe**
Financial	Nil	less than £100,000	between £100k and £250k	between £250k and £2.5m	greater than £2.5m
Reputational	Nil	Negligible adverse publicity. Minimal impact upon public perception	Localised adverse publicity. Minor / transient impact on public perception of Force or PCC	Criticism at local level. Lasting impact upon public perception of Force or PCC	Intense national media. Criticism at national level.
Operational	Nil	Negligible impact upon ability to deliver service and meet Force targets	Minor impact upon ability to deliver service and meet Force targets	Significant impact upon ability to deliver service and meet Force targets	Catastrophic impact upon ability to deliver service & meet Force targets
Legal / Compliance	Nil	Negligible prospect of legal challenge	Minor/Transient prospect of legal challenge	Serious non-compliance. Litigation/challenge	National legal issue

Overall Risk Score

Probability x Highest Impact = **Green** **/** **Amber** **/** **Red** Risk Status

Probability	Highly Probable	Nil	🟩	🟧	🟥	🟥
	Probable	Nil	🟩	🟩	🟧	🟥
	Unlikely	Nil	🟩	🟩	🟩	🟧
	Highly Improbable	Nil	🟩	🟩	🟩	🟩
	Nil	Nil	Nil	Nil	Nil	Nil
		Nil	Negligible	Minor	Significant	Severe
		Impact (choose your highest impact)				

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward @rsmuk.com

rsmuk.com