YORK AND NORTH YORKSHIRE COMBINED AUTHORITY - POLICE

Risk Management

FINAL Internal Audit Report: 1.26/27

17 July 2026

CONTENTS

Appendices

AUDIT OUTCOME OVERVIEW

Background / Why we did the audit

We have undertaken a review of the Force's risk management process. Our audit has considered the risk management policy, risk identification and escalation / de-escalation, risk matrix, controls, assurances, horizon scanning, opportunities and risk reporting to senior management. As part of our testing, we have looked at the overall Force Risk Register, a sample of Departmental Risk Registers and the Principal Risk Register.

Overall accountability for the risk management framework sits with the Risk Manager.

We confirmed that the Force has recently implemented a new risk management system, SmartCore, which went live on 1 June 2026. This system replaces previous arrangements and is intended to provide a more integrated, standardised platform for recording, monitoring, and reporting risks.

Conclusion:

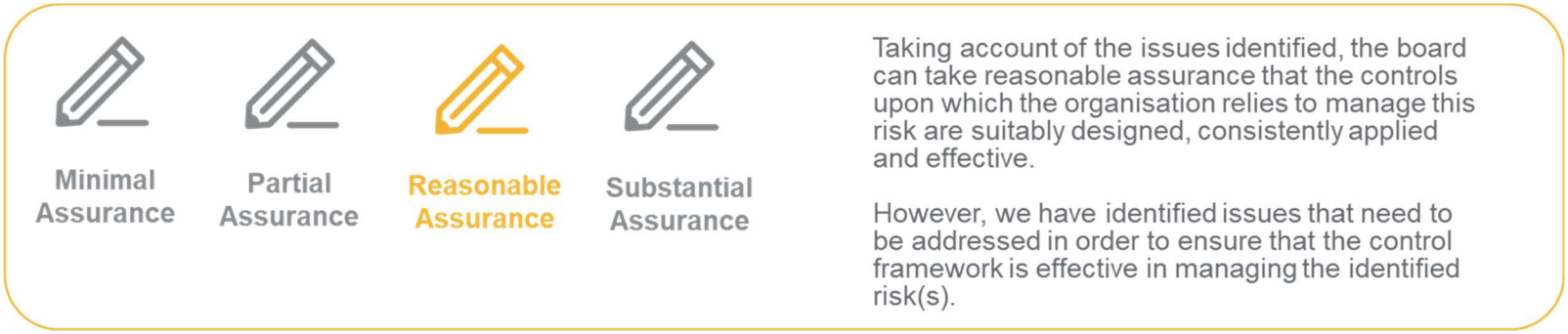
Our audit has identified that a process was in place to manage risk within the Force, supported by a policy and risk management software. We noted defined approaches to risk analysis and horizon scanning that support identifying risks, as well as an approach for capturing and assessing opportunities.

However, we did identify some areas for improvement, including considering the current format of the risk matrix to better differentiate between likelihood and impact, ensuring that high-impact risks are appropriately classified, prioritised, and subject to sufficient oversight. Additionally, there was a lack of documented, detailed controls and inherent risk scores. We also noted the size of the current departmental risk registers and identified that risk appetite was not explicitly discussed and reported to senior management.

The Force has been transitioning its approach, with a previous self service model moved to dedicated support through the Risk Manager. This has required evaluating processes and establishing more mature risk management methodology, which was still being developed at the time of the fieldwork and will reflect the root cause relating to a number of actions agreed.

As a result of our review, we have agreed **three low and four medium** priority management actions.

Internal audit opinion:



* Refer to Appendix B for more detail

Audit themes:

Our review identified the following issues resulting in the agreement of three low and three medium priority management actions:

Risk Management Policy and Procedures

The Force Risk Management Policy defines the risk register framework and clearly sets out roles, responsibilities, and accountability. It is in date, approved, and accessible to staff. We noted that the policy was last reviewed on 12 May 2026 and is scheduled for its next review on 28 February 2027. We obtained email approval of the policy dated 5 June 2026 from the Strategy and Governance Lead but did not see any formalised approval by a committee or board as part of our fieldwork. If the updated policy is not final, there is a risk that it may contain unapproved changes or inaccuracies, leading to inconsistent application and confusion over the correct procedures. **Low**

Risk Appetite

Supporting documents include a risk appetite statement and risk matrix procedure, with the Risk Matrix outlining how risks are identified, scored, managed, and escalated. However, risk appetite is not explicitly referenced in reports to key governance forums (Joint Independent Audit Committee, Strategic Oversight Board, and Risk, Assurance and Improvement Board), creating a risk that decisions are made without a consistent understanding of the level of risk the organisation is willing to accept, and/or whether the risk is within the appetite of the organisation. **Low**

Risk Matrix

We confirmed the Force have a 4 x 4 risk matrix in place. We did note that a score of nine is classified as green; however, this score reflects a scenario with severe impact, albeit highly improbable. Where risks with a severe impact are classified as ‘green’, there is a risk that they are deprioritised and do not receive appropriate visibility, scrutiny, or oversight, potentially resulting in insufficient focus on contingency planning and preparedness for high impact events. **Medium**

Force Risk Register

We confirmed there were currently 31 risks recorded on the Force Risk Register (FRR). Review of the current FRR confirmed that each risk has a description, nominated owner, review date, and both current and target scores. However, inherent risk scores are not recorded. The Risk Manager advised this is to maintain focus on current and target risk, although inclusion may be considered as the framework matures. The absence of inherent scoring limits visibility of unmitigated risk and may reduce the Force’s ability to assess control effectiveness and prioritise mitigation. **Medium**

Controls

We sampled 10 risks from the FRR and reviewed the associated risk reports. All included documented causes, effects, and actions with assigned owners and timeframes. Controls were recorded for six risks; however, four had no documented controls. Where controls are not recorded in SmartCore, there is a risk that mitigating measures are not clearly defined or effectively monitored.We also noted that controls and actions lacked detail, limiting clarity over their purpose and effectiveness and potentially impacting consistent application and oversight. **Medium x2**

Departmental Risk Register (DRR)

We reviewed five DRRs (Force Control Room, People Services, Information Management, Professional Standards, and Intelligence Analysts). Across all registers, each risk included a description, nominated owner, agreed timescale, and current and target scores. However, there was notable variation in the number of risks recorded. Intelligence Analysts and Professional Standards each had only two risks, while Information Management recorded 21. While the lower number for Intelligence Analysts reflects its smaller size, Professional Standards would typically be expected to hold more risks. There is a risk that some departmental registers may not fully or consistently capture the breadth of risks faced. **Low**

* Refer to Appendix B for more detail

Principal Risk Register

We confirmed that the Principal Risk Register (PRR) captures the Force's key risks as identified by senior management. Review of the current PRR confirmed eight risks are recorded, each with a description, nominated owner, agreed review timescale, and current and target scores. We obtained the risk report for all eight risks and confirmed in seven cases controls were documented. In the remaining case, we confirmed although actions had been identified, no controls were recorded. Where controls are not documented within SmartCore, there is a risk that mitigating measures are not clearly defined, consistently applied, or effectively monitored, which may impact the Force's ability to manage these risks appropriately. We have agreed an action for this in the 'Controls' section above.

We found the following control areas to be adequately designed and operating effectively:

Risk Identification

We obtained the portfolio assurance meeting reports for three separate department areas to confirm departmental risks are discussed to be proposed for escalation to the FRR at Risk, Assurance and Improvement Board (RAIB) and Strategic Oversight Board (SOB). In addition, we obtained the Risk Register and Business Continuity Overview Report presented to the Joint Independent Audit Committee (JIAC) in March 2026. Through review, we confirmed that the Committee receives updates on developments relating to the PRR, regarding the risks closed and risks added.

Horizon scanning

Review of RAIB reports from January, March, and May 2026 confirmed that horizon scanning is regularly considered. We verified that RSM produces an Emerging Risk Radar report, and that the Risk Manager contributes to the Police National Business Continuity Forum's Eye on the Horizon publication (December 2025). Attendance at the York and North Yorkshire Local Resilience Forum horizon scanning session (March 2026) further evidences engagement in identifying high-level risks that may impact partners and communities.

Opportunities

We obtained the Innovation Board Agenda from 14 May 2026, to confirm new opportunities are a standard agenda item. We obtained three example opportunity reports (out of 15 total) relating to allocating jobs from NICHE to team email boxes, AI, and Transactional Audit Automation (RPA). Review of three example opportunity reports (NICHE job allocation, AI, and RPA) showed each included a description, cause and consequences, review date, and current and target scores.

Risk escalation

Review of portfolio assurance meeting minutes across Protective Services, Organisational, and Local Policing and Safeguarding confirmed that risks are regularly discussed for potential escalation to the Force Risk Register via RAIB and SOB. Review of the last five SOB Risk Register Overview reports confirmed they provide risk management updates and a consolidated view of key escalated risks for senior oversight. RAIB reports from January, March, and May 2026 also evidence discussion of risks proposed for escalation to, and de-escalation or closure from, the FRR and PRR.

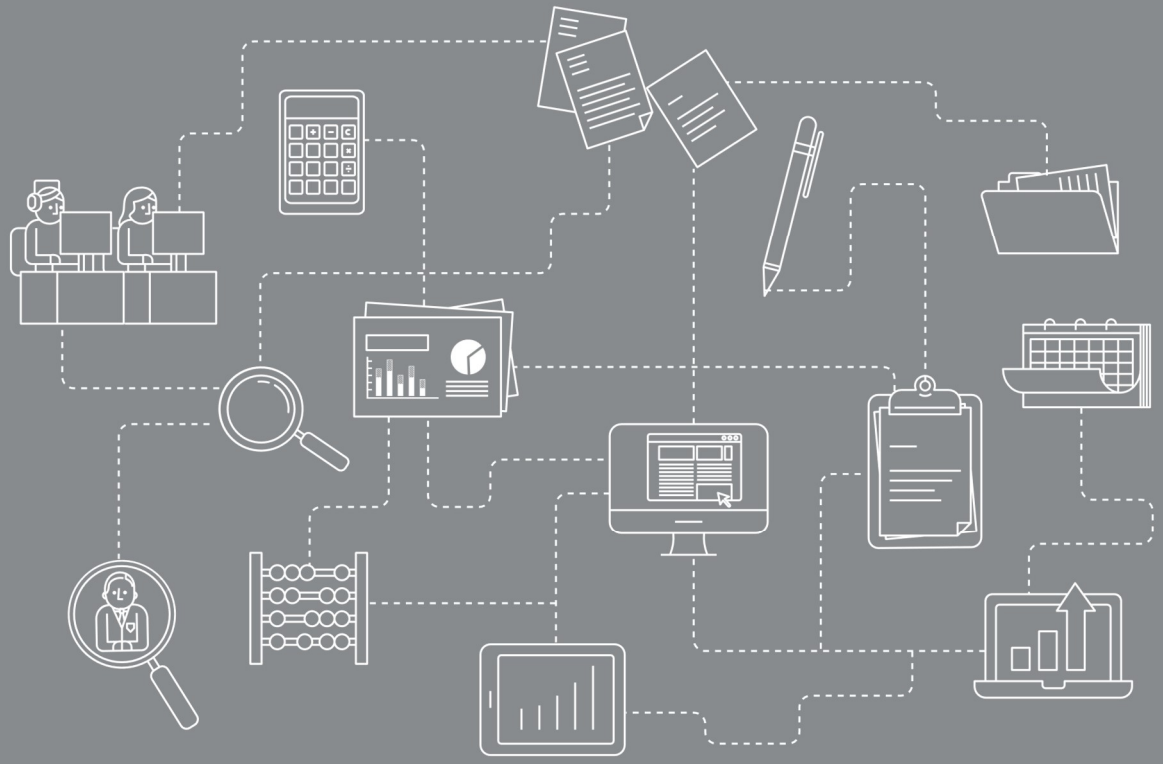
Assurances

We confirmed that reports are produced every two months for each Portfolio Assurance Board. Through review of the reports for three periods' worth of reports to three Portfolio Assurance Boards, we confirmed that the content within the reports covers how the Force are gaining assurance against the risks and key issues within each department. Whilst assurances are not formally documented against each risk, we have confirmed that assurances are discussed at a portfolio level with scrutiny from members of the Chief Officer Team.

* Refer to Appendix B for more detail

Summary of Actions for Management

01



SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High	Medium	Low
Immediate management attention is necessary.	Timely management attention is necessary.	There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
1	The Force will ensure that the final version of the Risk Management Policy is formally agreed, all tracked changes are removed, and the approved version is published and retained on file.	Low	Risk Manager	30 September 2026
2	The Force will agree a risk appetite statement for relevant areas, particularly for risks on the Force Risk Register. Following this, an approach will be agreed with RAIB to ensure formal reporting of risk scoring against risk appetite.	Medium	Risk Manager	31 March 2027
3	The Force will review and enhance its risk scoring methodology by considering a 5 x 5 risk matrix to better differentiate between likelihood and impact, ensuring that high-impact risks are appropriately classified, prioritised, and subject to sufficient oversight.	Medium	Risk Manager	31 March 2027
4	The Force will review whether it is beneficial to include an inherent risk score within the risk register framework. The result of this review will be communicated to an appropriate forum within the governance structure to enable oversight and challenge regarding the decision.	Low	Risk Manager	31 March 2027
5	The Force will implement regular checks (such as dip sampling) to confirm whether controls and actions have been documented for each risk. The Force will also investigate whether the risk management system can be updated to include a reminder or notification to ask risk owners whether they have added and updated all controls and actions.	Medium	Risk Manager	1 March 2027
6	The Force will develop guidance for expected levels of details needed for controls and actions. As above, the Force will implement regular checks (such as dip sampling) to confirm whether controls and actions are sufficiently detailed to clearly explain what the control and action is.	Medium	Risk Manager	1 March 2027
7	The volume of risks in departmental risk registers will be flagged internally and discussions held with owners of these risk registers to ensure that all relevant risks have been identified and recorded on the relevant register. The Force will target those departmental risk registers with a low volume of risks to determine whether this is accurate or whether additional risks can be recorded.	Low	Risk Manager	31 March 2027

* Refer to Appendix B for more detail

Detailed Findings and Actions

02

DETAILED FINDINGS AND ACTIONS

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 audit testing undertaken.

Area: Risk Management				
Control	The Force operates a Risk Management Policy, which sets out the Force's approach to risk management and risk appetite.		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	Through our review of the Force Risk Management Policy, we confirmed that it defines the Risk Register Framework, as well as roles, responsibilities, and accountability for risk management. We noted that the policy was last reviewed on 12 May 2026 and is scheduled for its next review on 28 February 2027. We obtained email approval of the policy dated 5 June 2026 from the Strategy and Governance Lead. However, we observed that this version was not final, as it still contained tracked changes. If the updated policy is not final, there is a risk that it may contain unapproved changes or inaccuracies, leading to inconsistent application and confusion over the correct procedures.			
Management Action 1	The Force will ensure that the final version of the Risk Management Policy is formally agreed, all tracked changes are removed, and the approved version is published and retained on file.	**Responsible Owner:** Risk Manager	**Date:** 30 September 2026	**Priority:** **Low**

Area: Risk Appetite				
Control	There is a risk appetite document in place that forms part of the Risk Management Policy.		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	We reviewed the Risk Appetite document and confirmed that it outlines the Force's risk appetite, strategic risks, the risk tolerance process, and escalation procedures. We noted that risks are categorised into three risk appetite groups: • **Categories 1 and 2 (Red):** Notify the line manager and consider discussing with senior colleagues. Ensure the risk is reviewed within one month and escalate it to the Portfolio Assurance Meetings; • **Categories 3 and 4 (Amber):** Consider discussing the risk with the line manager and ensure it is reviewed within three months; and • **Categories 5 and 6 (Green):** Monitor for any changes and ensure the risk is reviewed within five months. Whilst the risk appetite statement sets out that the Force has a 'risk conscious culture', we did note that there are no specific risk appetite statements (either at an individual or thematic level).			

Area: Risk Appetite				
	Whilst the risk appetite groups and categories noted above indicate that there is an approach in place, this is a blanket approach for all risks and does not allow for the Force to accept additional risk in areas where this is appropriate. For example, there could be risk areas or themes in which the Force is more willing to accept risk, however this would not be compatible with the current approach to risk appetite. We also noted that, other than the risk appetite document, risk appetite is not explicitly referenced within reports to the Joint Independent Audit Committee, Strategic Oversight Board and Risk, Assurance and Improvement Board. If risk appetite is not outlined and reported to relevant governance forums, there is a risk that decisions are made without a consistent understanding of the level of risk the organisation is willing to accept.			
Management Action 2	The Force will agree a risk appetite statement for relevant areas, particularly for risks on the Force Risk Register. Following this, an approach will be agreed with RAIB to ensure formal reporting of risk scoring against risk appetite.	**Responsible Owner:** Risk Manager	**Date:** 31 March 2027	**Priority:** Low

Area: Risk Matrix			
Control	There is an approved risk matrix in place, which is used to score risks based on probability and impact.	**Assessment:**	
		Design	×
		Compliance	-
Findings / Implications	Through review of the risk matrix procedure, we confirmed that a 4 x 4 risk matrix is used to assess the risk and calculate the risks overall score. We noted that risks are scored based on impact and probability, which is standard practice within risk management. The Risk Manager advised that the risk matrix does not have a separate approval process as it is approved as part of the annual approval of the Risk Management Policy. We obtained the current risk matrix used by the force and confirmed that risks are scored on a scale from one to 16, where one represents 'highly improbable' risks with 'negligible impact', and 16 represents 'highly probable' risks with 'severe impact'. We observed the following classifications: • Scores one to 10 are classified as green; • Scores 11 to 13 are classified as amber; and • Scores 14 to 16 are classified as red. We noted that a score of nine is classified as green, even though this represents a risk with 'severe impact' (the highest impact score) and 'highly improbably' probability. Definitions of 'severe impact' include: • financial impact of greater than £2.5m; • intense national media and criticism at national level; • catastrophic impact upon ability to deliver service and meet Force targets; or • national legal issue. Given the definitions of a severe impact, it could be beneficial for the Force to review whether the current matrix is fit for purpose, or whether a 5 x 5 risk matrix with updated RAG ratings would be more appropriate. Where risks with a severe impact are classified as 'green', there is a risk that they may not receive the appropriate visibility, scrutiny or oversight required, potentially resulting in insufficient focus on contingency planning and preparedness for high impact events. We obtained the FRR, PRR and five DRRs and through review we confirmed risks are scored in accordance with the approved risk matrix.		

Area: Risk Matrix				
Management Action 3	The Force will review and enhance its risk scoring methodology by considering a 5 x 5 risk matrix to better differentiate between likelihood and impact, ensuring that high-impact risks are appropriately classified, prioritised, and subject to sufficient oversight.	**Responsible Owner:** Risk Manager	**Date:** 31 March 2027	**Priority:** Low

Area: Force Risk Register			
Control	Where DRRs contain risks that are outside of the department's tolerance to manage, they are escalated to the FRR by Department Heads, subject to review by the Risk Manager.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	We confirmed that the FRR captures all escalated risks from DRRs requiring Force level oversight, with 31 risks currently recorded. Discussion with the Risk Manager highlighted that the cause of the volume of risks was due to a number of compliance issues being identified, and to ensure transparency and appropriate monitoring, a decision was made to record each of the issues within the FRR. We were advised that this is a temporary measure and the Force is in the process of reducing the number of risks once these compliance issues are resolved. Management advised the focus on transparency and appropriate monitoring has been directed from the Chief Officer Team, and that there is an acceptance of more risks to ensure greater scrutiny compared to less risks and a more streamlined risk register. We noted that the Force does not record an inherent risk score for each risk. We raised this with the Risk Manager, who explained that a decision had been made to exclude inherent scoring in order to maintain focus on current and residual risk scores. However, it was acknowledged that, as the risk management process matures, the inclusion of inherent risk scores is something the Force would be looking to include. Where the inherent risk score is not recorded on the risk register, there is a risk that the organisation lacks visibility of the true, unmitigated level of risk exposure. This may limit its ability to assess the effectiveness of existing controls, prioritise risks appropriately, and make informed decisions about where additional mitigation is required.		
Management Action 4	The Fore will review whether it is beneficial to include an inherent risk score within the risk register framework. The result of this review will be communicated to an appropriate forum within the governance structure to enable oversight and challenge regarding the decision.	**Responsible Owner:** Risk Manager	**Date:** 31 March 2027	**Priority:** Low

Area: Controls			
Control	Risk reports for each risk are held within the SmartCore system, which detail the controls and actions for each risk.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	We selected a sample of 10 risks from the FRR and obtained the corresponding risk report for each. For all risks reviewed, we confirmed that causes and effects were documented, and that actions were in place with agreed owners and timeframes. Additionally, for six of the 10 risks, we confirmed that controls had been documented with agreed owners and timeframes. However, for the remaining four risks although actions had been identified, no controls were recorded.		

Area: Controls				
	Where controls are not documented within SmartCore, there is a risk that mitigating measures are not clearly defined, consistently applied, or effectively monitored, which may impact the Force's ability to manage these risks appropriately or ensure they are effective. We also noted instances where controls and actions were not documented in detail. For example, for risk 9236, one control was listed as 'IOPC Feedback Report' and one action as 'Dashboard', with no further explanation. Where controls and actions are not clearly or comprehensively described, there is a risk that their purpose, implementation, and effectiveness are not fully understood, which may limit the organisation's ability to consistently apply and monitor these measures.			
Management Action 5	The Force will implement regular checks (such as dip sampling) to confirm whether controls and actions have been documented for each risk, as well as whether they clearly explain what the control and action is. The Force will also investigate whether the risk management system can be updated to include a reminder or notification to ask risk owners whether they have added and updated all controls and actions.	**Responsible Owner:** Risk Manager	**Date:** 1 March 2027	**Priority:** Medium
Management Action 6	The Force will develop guidance for expected levels of details needed for controls and actions. As above, the Force will implement regular checks (such as dip sampling) to confirm whether controls and actions are sufficiently detailed to clearly explain what the control and action is.	**Responsible Owner:** Risk Manager	**Date:** 1 March 2027	**Priority:** Medium

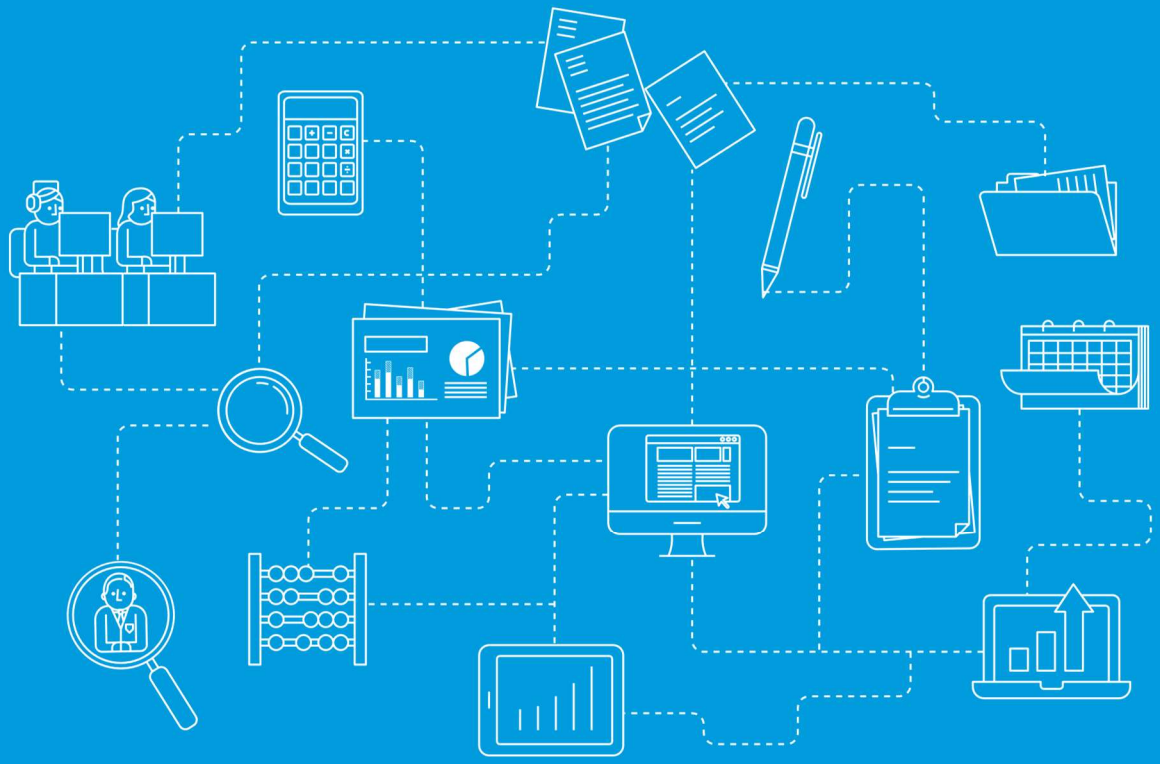
Area: Departmental Risk Register			
Control	Each department area has a separate risk register. Risks from the DRR are escalated to the FRR and PRR.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	We selected a sample of five DRRs (Force Control Room, People Services, Information Management, Professional Standards and Intel Analysts). Through review of all five we confirmed for each risk: • there is a risk description; • there is a nominated risk owner for each risk; • a timescale for completion has been agreed for each risk; and • there is a current and target score for each risk. However, we observed some variation in the number of risks recorded across DRRs For example, both the Intelligence Analysts and Professional Standards register's contained only two risks each, while the Information Management register included 21 risks. This was queried with the Risk Manager, who confirmed that the Intelligence Analysts function is relatively small and would therefore be expected to have a limited number of risks. If there are only a small number of risks recorded within DRRs, there is a risk that these registers do not consistently or comprehensively reflect the full range of risks faced by each function.		

Area: Departmental Risk Register				
Management Action 7	The volume of risks in departmental risk registers will be flagged internally and discussions held with owners of these risk registers to ensure that all relevant risks have been identified and recorded on the relevant register. The Force will target those departmental risk registers with a low volume of risks to determine whether this is accurate or whether additional risks can be recorded.	**Responsible Owner:** Risk Manager	**Date:** 31 March 2027	**Priority:** Low

Area: Principal Risk Register			
Control	The PRR is in place to hold the most significant elements of uncertainty as determined by the executive. Risks from the FRR and DRR are escalated to the PRR.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	We confirmed that the PRR documents the Force's most important risks, as identified by senior management. Through review of the PRR from May 2026, we confirmed there are currently eight risks. We verified that the PRR is also incorporated into the reporting arrangements through the Force's governance structure, including to the RAIB. We confirmed for each risk: • there is a risk description; • there is a nominated risk owner for each risk; • a timescale for review has been agreed for each risk; and • there is a current and target score for each risk. We also obtained the risk report for all eight risks and confirmed in seven cases controls were documented. In the remaining case, we confirmed although actions had been identified, no controls were recorded. Where controls are not documented within SmartCore, there is a risk that mitigating measures are not clearly defined, consistently applied, or effectively monitored, which may impact the Force's ability to manage these risks appropriately. We have raised an action for this in an above control.		
	See management action 5		

Appendices

03



APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings

Low

There is scope for enhancing control or improving efficiency.

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 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 following table highlights the number and categories of management actions made as a result of this audit.

Area	Control design not effective*	Non-compliance with controls*	Agreed actions		
			Low	Medium	High
Risk Management Policy and Procedures	0 (1)	1 (1)	1	0	0
Risk Appetite	0 (1)	1 (1)	1	0	0
Risk Identification	0 (1)	0 (1)	0	0	0
Risk Matrix	0 (1)	1 (1)	0	1	0
Horizon scanning	0 (1)	0 (1)	0	0	0
Opportunities	0 (1)	0 (1)	0	0	0
Force Risk Register	0 (1)	1 (1)	0	1	0
Controls	0 (1)	1 (1)	0	2	0
Departmental Risk Registers	0 (1)	1 (1)	1	0	0
Principal Risk Register	0 (1)	0 (1)	0	0	0
Risk escalation	0 (1)	0 (1)	0	0	0
Assurances	0 (1)	0 (1)	0	0	0
Total			**3**	**4**	**0**

* 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

APPENDIX B: INTERNAL AUDIT ASSIGNMENT OPINIONS

Minimal Assurance

Taking account of the issues identified, the board cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Urgent action is needed to strengthen the control framework to manage the identified risk(s).

Reasonable Assurance

Taking account of the issues identified, the board can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk(s).

Partial Assurance

Taking account of the issues identified, the board can take partial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Action is needed to strengthen the control framework to manage the identified risk(s).

Substantial Assurance

Taking account of the issues identified, the board can take substantial assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.

Debrief held	19 June 2026	**Internal audit Contacts**	Dan Harris, Head of Internal Audit Matthew Stacey, Managing Consultant Ella Robson, Consultant
Draft report issued	3 July 2026		
Responses received	17 July 2026		
Final report issued	17 July 2026	**Client sponsor**	Strategy and Governance Lead
		Distribution	Risk Manager Strategy and Governance Lead

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com.

rsmuk.com