CROYDON

Final Internal Audit Report

Risk Management

September 2025

Distribution: Head of Insurance, Anti-Fraud & Risk
Governance Officer
Director of Finance & Deputy S151 Officer
Corporate Director of Resources & S151 Officer

Assurance Level	Issues Identified	
Substantial	Priority 1	0
	Priority 2	4
	Priority 3	0

forvis mazars

Contents

Page

Executive Summary

Detailed Report

Appendices

1. Introduction

1.1 A robust and effective risk management framework to identify, mitigate and monitor key risks which have the potential to impact the achievement of strategic objectives is essential for all local authorities.

1.2 Given reductions in funding over several years leading to financial sustainability issues, operational challenges and additional regulatory scrutiny of local authorities, effective risk management frameworks and processes are crucial in ensuring that services are successfully delivered and that public trust is maintained. Through the proactive identification and effective management of key risks, Croydon Council (the Council) can minimise its financial and regulatory exposure and help ensure that resources are efficiently utilised to aid the achievement of strategic objectives and minimise the likelihood of service disruption.

1.3 The Council's *Practical Guide to Risk Management* (Guide) provides insight into the Council's strategy and approach towards risk management. As outlined within the Guide, the Council uses a 5x5 probability-impact matrix to calculate a risk rating; where any rating above 20 is deemed as high-risk which requires immediate management and monitoring.

1.4 Following the identification of a risk, the Council uses its risk management software, JCAD, to record details of the risk, potential impact if the risk was to crystallise, current risk rating and future risk rating. Alongside these details, risk owners are assigned in JCAD to manage the risk, typically either Corporate Directors, Directors or Head of Service. To justify the current and future risk ratings calculated, risk owners are required to document the current control measures in place to mitigate the risk and the future control measures which the Council plans to implement.

1.5 All risks recorded within JCAD are required to be subject to a three-month review cycle, where risk owners are responsible for reviewing the risk details to confirm that the risks remain relevant and that the information, such as potential impact and control measures, remains accurate. To improve the oversight of risks within operational teams, the Council developed a Power BI dashboard which is integrated with JCAD and allows for heads of service to access live risk information, so that risk management can be actively embedded into day-to-day operations.

1.6 Directorate Management Teams (DMT) are responsible for completing quarterly reviews of all risks related to their directorate, where the Head of Fraud, Risk & Insurance provides the risk summary and risk detail reports for discussion during the meetings. Within the guide, DMTs are also responsible for ensuring that emerging risks are promptly identified and proactively recorded within JCAD.

1.7 Risk information is provided to the Corporate Management Team (CMT) on a monthly basis. Following CMT discussions, the Council has identified strategic

risks which are to be monitored closely as these require the involvement of multiple directorates.

1.8 Risk Summary and Risk Detail reports, with an extract of all risks from JCAD are also provided to Audit & Governance Committee (AGC) on a quarterly basis. This provides the AGC with the opportunity to scrutinise risk management and select risks to be scrutinised further within risk 'deep dives;' where the corporate risk owner is responsible for presenting details of the risk, the mitigations in place, and to provide a summary of the future controls to be embedded.

1.9 Risk management forms a core component of the Annual Governance Statement (AGS) published alongside the Council's Financial Statements. The Accounts and Audit Regulations 2015 require each English local authority to conduct an annual review of the effectiveness of its system of internal controls and publish an AGS. In the context of the challenges faced by the Council, the last AGS published was in 2020/21.

1.10 This audit was part of the agreed Internal Audit Plan for 2024/25. The Terms of Reference and agreed scope for this audit is included under Appendix 1.

2. Key Issues

Priority 2 Issues
Sample testing of ten risks selected from JCAD identified three instances where risk owners had not evidenced a review of the risk within the last quarter. **(Issue 1)**
Sample testing of ten risks (and review of the current and future risk ratings and controls documented within JCAD) identified: • One instance where the level of detail recorded for current and future controls was not commensurate with the current and future risk ratings applied; • One instance where there had been a decrease in the future risk rating when compared to the current risk rating; however, the future controls or narrative to justify the reduction in risk rating had not been documented; and • One instance where the implementation date for a future control had been surpassed and had not been updated to reflect when the control will be implemented by. **(Issue 2)**
The Council had not documented a risk appetite statement which is used to inform strategic decision making. **(Issue 3)**
Examination of the three most recent quarterly DMT meeting minutes was unable to assess the depth of discussions held over the adequacy/accuracy of risk information recorded within JCAD, and that consideration had been given to any emerging risks/potential risks which had not already been recorded within JCAD. **(Issue 4)**

There were no Priority 3 findings.

3. Actions and Key Findings/Rationale

Control Area 2: Use of Risk Registers for Management & Ownership of Risks

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 1
2	Risk Champions to have their attention drawn to this finding. JCAD automation of risk reminders is weekly and risk champions are copied in. Technically a risk is 'overdue' on JCAD from the 1st day of the new quarter but in practice no one is expected to sign off on this date so if it is reviewed and signed off in the quarter before the Corporate Director reviews then it is compliant, ie up to 90 days after the 'due' date.	**Expected Control** As outlined within the *Risk Management Practical Guide*, risks recorded within JCAD are reviewed on a quarterly basis by their assigned risk owners, to ensure that the probability and impact assessments of risk crystallising remain accurate. **Finding/Issue** A sample of ten risks was selected from JCAD to confirm that the assigned risk owners had completed a review of each risk within the last quarter and that a clear audit trail was maintained within JCAD. The following issues were identified: • Ref.PST0012 – the risk had last been reviewed 5 July 2024 and was due for review 1 October 2024. Thus, the risk was overdue for review by 140 days as of the first day of audit fieldwork (17 February 2025); • Ref.CEHR0076 – the risk had last been reviewed 1 October 2024 and was due for review 1 January 2025. Thus, the risk was overdue for review by 48 days as of the first day of audit fieldwork (17 February 2025); and • Ref.HOTS0010 – the risk had last been reviewed 6 November 2024 and was due for review 1 January 2025. Thus, the risk was overdue for review by 48 days as of the first day of audit fieldwork (17 February 2025).

		The Head of Fraud, Risk & Insurance advised that JCAD produces automated notifications which were sent to risk owners on a weekly basis to highlight risks which are overdue for review. As a result, the owners of the risks listed above should have received several reminders by the time of audit. Additionally, overdue risk reviews were highlighted by the Head of Fraud, Risk & Insurance within emails sent to directors prior to quarterly DMT meetings, and it was confirmed that these emails had been sent for the most recent quarterly DMT meetings. Internal Audit were unable to verify whether these had been discussed and actioned subsequent to the DMT meetings. **Risk** Where risks are not reviewed on a regular basis in the line with the Council's policy, there is potential that the Council fails to identify changes to the probability or potential impact of risks crystalising and fails to implement additional control measures where this is required.
Responsible Officer	Deadline	
Head of Fraud, Risk & Insurance	1 July 2025	

Control Area 2: Use of Risk Registers for Management & Ownership of Risks

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 2
2	Risk Champions to have their attention drawn to this finding. These are challenged at DMTs, and the one-page scoring guide is used to help risk owners to be consistent, although we accept, we will never achieve 100% consistency, we strive for it.	**Expected Control** Corporate risks recorded within JCAD include information on the current control measures in place to mitigate the probability and potential impact of risks crystallising. Where there is a difference between the current and future risk rating applied, future control measures are outlined which are commensurate with the current and future risk ratings and have clear implementation dates recorded within JCAD. **Finding/Issue** Examination of a sample of ten corporate risks selected from JCAD identified the following: • Ref.CDS0021 – Both the current and future risk ratings recorded within JCAD were Medium (scored 9 out of 25). However, only one current control measure *(Improvement plan for organisational information governance)* was listed, compared to an additional nine future control measures, which would suggest that either sufficient information on the current control measures had not been recorded, or that the current or future risk rating applied was inaccurate; • Ref.HOTS0010 – The current risk rating applied within JCAD was Medium (9 out of 25) and the future risk rating was Low (6 out of 25). However, no additional future controls or narrative had been recorded to justify the reduction in the future risk rating, and • Ref.PH0002 – Future controls were documented within JCAD; however, the future implementation date (1 September 2024) had been surpassed, and the risks had

Responsible Officer	Deadline	
Head of Fraud, Risk & Insurance	1 July 2025	not been updated as current controls during the most recent risk review completed 17 January 2024. **Risk** Due to insufficient or outdated information recorded within JCAD for current and future controls, there is a lack of transparency and clarity over the current and future risk ratings applied. This can potentially impact the Council's ability to scrutinise corporate risks and control measures, and lead to instances where the Council fails to promptly implement sufficient mitigating control measures.

Control Area 3: Risk Appetite

<table>
<tr><th>Priority</th><th>Action Proposed by Management</th><th>Detailed Finding/Rationale - Issue 3</th></tr>
<tr><td>2</td><td>Agreed. This is being delivered as part of the review of the Transformation/Stabilisation Plan to fully articulate and reflect back the Councils appetite for risk associated with change.</td><td rowspan="3">Expected Control
A risk appetite statement has been issued which clearly defines the types and degree of risk the Council is willing to tolerate within key strategic areas. The risk appetite statement is utilised during the decision-making process to evaluate new opportunities/projects, to ensure that Council activities are aligned with strategic objectives and ensure that adequate controls have been put in place to mitigate risks in line with the Council's risk appetite.
Finding/Issue
The Head of Fraud, Risk & Insurance explained that the Council had not yet prepared a risk appetite statement, though it was something was being considered.
In addition, the Head of Fraud, Risk & Insurance reported that the Council would be implementing a new approach where the risk profile of new projects/strategic opportunities was to be calculated using a 5x5 risk matrix (Impact x Probability) similarly to how risks are currently assessed in JCAD. The calculated risk profile of each opportunity will be reported to Improvement and Assurance Panel (IAP) for review, alongside project business cases, to help ensure that decision making reflects the potential risks and benefits of opportunities.
Risk
As the Council's tolerance and appetite towards accepting risks has not been formally documented, there is a risk that this can lead to lack of clarity over strategic direction, the acceptance of inappropriate and intolerable risks, and result in the Council failing to achieve its strategic objectives.</td></tr>
<tr><th colspan="2">Responsible Officer</th><th>Deadline</th></tr>
<tr><td colspan="2">Head of Fraud, Risk & Insurance</td><td>August 2025</td></tr>
</table>

Control Area 5: Identification and Management of Emerging Risks (incl. Benchmarking) / Control Area 6: Monitoring and Reporting

Priority	Action Proposed by Management	Detailed Finding/Rationale - Issue 4
2	This will be drawn to the attention of the note takers for the Corporate Directors.	**Expected Control** The Council's *Practical Guide to Risk Management* outlines that Corporate Directors and Directors are responsible for meeting quarterly with their DMTs to review the adequacy of the risks recorded and to ensure that emerging risks are recorded within JCAD. **Finding/Issue** Review of respective DMT minutes and the three most recent Risk Detail Reports provided to DMTs (for Q2, Q3 and Q4 of the financial year 2024/25), where the Head of Fraud, Risk & Insurance provided each directorate with quarterly information regarding the risks relevant to their directorate and highlighted instances of overdue risk reviews and issues related to the risk details recorded within JCAD, confirmed that DMTs had discussed risks quarterly. However, the level of detail in some of the DMT minutes did not properly evidence whether: • The risks had been reviewed (for ASCH and Housing), • Discussions over the completeness of risk registers, i.e. whether there were any new or emerging risks which had not been captured within JCAD (for Children, Young People and Education (CYPE); Assistant Chief Executive (ACE); and

Responsible Officer	Deadline	
Head of Fraud, Risk & Insurance	July 2025	Sustainable Communities, Regeneration and Economic Recovery (SCRER)), had occurred. **Risk** DMTs do not apply appropriate scrutiny over the risks and control measures recorded within their directorates and potentially fail to identify emerging risks, leading to the Council failing to implement appropriate measures to effectively manage risks and prevent risks from materialising.

Appendix 1

AUDIT TERMS OF REFERENCE

Risk Management

1. INTRODUCTION

1.1 An effective risk management is essential for any organisation to ensure that it can continue to operate and deliver its objectives through uncertainty. A risk management framework should include mechanisms to identify and assess threats and ensure controls have been put in place to reduce risks to an acceptable level. The organisation should have defined its appetite for risks to allow it to determine the level of controls required. Risks should be recorded and subject to ongoing monitoring, and an awareness of risk should be embedded in the organisation's working culture.

1.2 Local authorities have faced increased exposure to financial risks in recent years, due to funding pressures, COVID-19, and underperforming commercial investments: while between 1988 and 2018, only two Section 114 notices were issued by under the Local Government Finance Act 1988, there have been ten since 2018. This has highlighted the need for careful financial risk management in the local government sector.

1.3 Croydon Council has a Risk Management Practical Guide on the Council's intranet which sets out the broader risk management framework, which includes a Risk Statement. The Council maintains a single integrated corporate risk register using JCAD software – all risks, both corporate and departmental, should be captured in JCAD and there are no separate departmental risk registers. All risks have an owner, which is normally a Corporate Director, Director or Head of Service, who is responsible for managing the risk. The register also includes strategic risks which require a cross-cutting approach directed by Corporate Management Team (CMT).

1.4 The Council does not have a Risk Appetite Statement, but this is currently under discussion. At present, risks are assessed using a 5x5 probability-impact matrix to give a risk score out of 25, with any score over 20 considered beyond tolerance.

1.5 The Head of Fraud, Risk & Insurance undertakes a quarterly exercise with each Corporate Director to identify new and emerging risks, which are added to the register accordingly. In addition, the Council has recently worked with an external consultant from JCAD to undertake external benchmarking.

1.6 Each directorate in the Council has a designated risk champion who coordinates between the Head of Fraud, Risk & Insurance. The Head of Fraud, Risk and Insurance reports on risks regularly to the Audit & Risk Committee (ARC), CMT and Mayor's Advisory Board (MAB).

1.7 An audit of risk management at Croydon Council was last undertaken in the financial year 2019/20. Since then, there have been significant changes to the risk environment in Croydon and local government more broadly, including the

Council's exposure to financial risks as highlighted by the Report in the Public Interest 2020 and precarious financial position underlined by Section 114 notices issued in November 2020, December 2020 and November 2022.

1.8 This audit was part of the agreed Internal Audit Plan for 2024/25.

2. OBJECTIVES AND METHOD

2.1 The overall audit objective was to provide an objective independent opinion on the adequacy and effectiveness of controls / processes.

2.2 The audit for each control / process being considered:

- Walked-through the processes to consider the key controls;
- Conducted sample testing of the identified key controls, and
- Reported on these accordingly.

3. SCOPE

3.1 This audit, focused on assessing whether Croydon Council has in place adequate and appropriate policies, procedures, and controls to manage the Virtual Wallet was undertaken as part of the 2024/25 Internal Audit Plan. The specific scope included the following areas and recommendations:

Control Areas/Risks	Issues Raised		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Legislative, Organisational and Management Requirements (Risk Management Framework)	0	0	0
Use of Risk Register for Management & Ownership of Risks	0	2	0
Risk Appetite	0	1	0
Embedding of Risk within the Council (incl. Training, Roles & Responsibilities)	0	0	0
Identification and Management of Emerging Risks (incl. Benchmarking)	0	1*	0
Monitoring and Reporting	0	1*	0
Total	**0**	**4**	**0**

*This is a single issue that applies to two scope areas, so has only been counted once in the total

Appendix 2

Definitions for Audit Opinions and Identified Issues

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives, and the controls are constantly applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance of the controls which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and non-compliance that puts achieving the system objectives at risk,
	No Assurance	Controls are non-existent or extremely weak, leaving the system open to the high risk of error, abuse, and reputational damage.

Priorities assigned to identified issues are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require immediate attention by management to action and mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that still represent an exposure to risk and need to be addressed within a reasonable period.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, still provides an opportunity for improvement. May also apply to areas considered to be of best practice that can improve for example the value for money of the review area.

Statement of Responsibility

We take responsibility to London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work 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. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.