



SLOUGH BOROUGH COUNCIL

Internal Audit Progress Report

For the Audit and Corporate Governance
Committee meeting on 28 July 2022

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.



1 KEY MESSAGES

The internal audit plan for 2021/22 was approved by the Audit and Corporate Governance Committee (ACGC) at the March 2021 meeting, with the revised plan being approved at the July 2021 meeting.

The 2022/23 draft internal audit plan was discussed at the March 2022 ACGC and it was agreed that some further amendments to that plan would be agreed with the Director of Finance. These discussions were held immediately after the March meeting and the amendments agreed and the revised 2022/23 plan is on the July 2022 ACGC meeting agenda.

This section provides an update on the key messages relating to the progress of the 2021/22 and 2022/23 plans.

2021/22 Internal Audit Plan



We have issued a further seven final reports since the March 2022 Audit and Corporate Governance Committee meeting. Of these, two have resulted in a 'Minimal' (negative) assurance opinion, two resulted in a 'Partial' (negative) assurance opinion and the remaining three were Advisory reports. It should be noted that significant control weaknesses were identified for all three advisory reviews and all seven of these final reports have impacted and contributed to our year end opinion. Further details on these reports are documented below. [\[To note\]](#)

We have also issued a further 15 draft reports and we are waiting for management responses to all of these before they are finalised and presented to the Committee.

2022/23 Internal Audit Plan



The 2022/23 Internal Audit Plan is underway with one report issued in draft and two reviews where the fieldwork is complete ahead of draft reports being issued. Two further reviews are currently in progress. [\[To note\]](#)

2021/22 Head of Internal Audit Opinion



We advised the Committee at the March 2022 meeting that we would be issuing a negative Head of Internal Audit opinion for 2021/22, given the outcomes of our audits at that point. We have issued a number of additional reports in draft since the last meeting with negative opinions where we have found weaknesses to still be present. We have provided further updates to the S151 officer and monitoring Officer at our regular meetings. The 2021/22 opinion is on the agenda as part of our annual report. [\[To note\]](#)

The Committee will need to continue to carefully monitor the progress made by Officers to implement the management actions agreed from the 2021/22 and previous years Internal Audit reviews. [\[To note\]](#)

Please note that historically, the Risk and Audit board, audit sponsor, S151 Officer, Chief Executive and Chair of this Committee received a copy of all final reports issued throughout the year as they were finalised (as in previous years). This process has been revised during 2021/22 and we understand the Director of Finance (S151) provides copies of the final reports to the Chair of this committee. [\[To note\]](#)



2 INTRODUCTION

This report provides a summary update on progress against the remaining audits from the 2020/21 internal audit plan and progress against the 2021/22 and 2022/23 plans. The report is based on the position as at the 19th July 2022.

2020/21 Internal Audit Plan

Since the last audit committee in December 2021, one report remains in draft relating to the 2020/21 audit plan:

- Follow Up Q4 – Little progress – responses have been received from the Council, we have amended the draft report and re-issued a revised draft and we are liaising with officers to finalise this report.

2021/22 Internal Audit Plan

The Internal Audit Plan for 2021/22 was approved by the Audit and Corporate Governance Committee initially on 4th March 2021, and a revised plan was subsequently approved on 29th July 2021. Since the last update provided in March 2022, the following seven reports have been finalised:

- Supplier Duplicate Payments – Advisory (but significant weaknesses)
- Temporary Accommodation – Minimal Assurance
- Risk Management – Partial Assurance
- Capital Expenditure – Partial Assurance
- General Data Protection Regulation (GDPR) Governance – Advisory (but significant weaknesses)
- Creditors – Minimal Assurance
- Cyber Essentials – Advisory (but significant weaknesses)

In addition, we have issued the following 15 reports in draft from the Internal Audit Plan for 2021/22. It should be noted that these reviews are still in draft and are with management for comment:

- Follow Up of Previous Management Actions Quarter 2 – Issued 24th September 2021
- Payroll – Issued 9th November 2021
- Assets – Issued 31st January 2022
- Business Rates – Issued 21 February 2022
- Follow Up of Previous Management Actions Quarter 3 – Issued 7 March 2022
- Schools Audit – Priory School – Issued 24 March 2022
- RMI Contract Management – Osborne – Issued 11 April 2022
- Health and Safety – Issued 28 April 2022
- Matrix – Management of Agency Staff – Issued 28 April 2022
- IDEA – Supplier Duplicate Payments – Phase 2 – Issued 3 May 2022
- Follow Up of Previous Management Actions Quarter 4 – Issued 12 May 2022
- Capital Projects – Britwell Expansion – Issued 13 May 2022
- Slough Children First – Governance – Issued 16 May 2022

- 
- Leasehold Service Charges – Issued 18 May 2022
 - Slough Children First – Value for Money – Issued 14 June 2022

2022/23 Internal Audit Plan

At this stage the audit plan is underway with one draft issued, two reviews complete and draft reports will be issued shortly, and two reviews have fieldwork in progress. No final reports have been issued.

3 OTHER MATTERS

3.1 Changes to the plan

The following changes were agreed since the last meeting:

Note	Auditable area	Reason for change
1	Subsidiary Governance	Following discussions with the Director of Finance, we have agreed to move the Subsidiary Governance review from the 2021/22 plan to the 2022/23 plan.

Quality assurance and continual improvement

To ensure that RSM remains compliant with the IIA standards and the financial services recommendations for Internal Audit we have a dedicated internal Quality Assurance Team who undertake a programme of reviews to ensure the quality of our audit assignments. This is applicable to all Heads of Internal Audit, where a sample of their clients will be reviewed. Any findings from these reviews being used to inform the training needs of our audit teams. The Quality Assurance Team is made up of; the Head of the Quality Assurance Department (FCA qualified) and an Associate Director (FCCA qualified), with support from other team members across the department. This is in addition to any feedback we receive from our post assignment surveys, client feedback, appraisal processes and training needs assessments.

External reviews of quality

One of the key measures of quality is an independent third-party assessment and, as a firm we are required to conform to the requirements of the International Professional Practices Framework (IPPF) published by the Global IIA. Under the Standards, internal audit services are required to have an external quality assessment (EQA) every five years. The RSM UK Risk Assurance service line commissioned an external independent review of our internal audit services in 2021, to provide assurance as to whether our approach continues to meet the requirements.

The external review concluded that RSM 'generally conforms to the requirements of the IIA Standards' and that 'RSM IA also generally conforms with the other Professional Standards and the IIA Code of Ethics. There were no instances of non-conformance with any of the Professional Standards'.

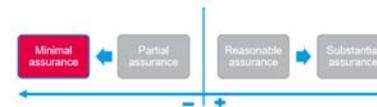
The rating of 'generally conforms' is the highest rating that can be achieved, in line with the IIA's EQA assessment model.

APPENDIX A - KEY FINDINGS FROM FINALISED 2021/22 INTERNAL AUDIT REPORTS

Detailed below are the High and Medium Priority Management Actions from negative opinion reports i.e. **Partial or Minimal Assurance reports** (or **Poor or Little progress** for follow up reports) and any **advisory reviews where significant issues were identified** (in the exception format previously agreed by the Committee):

Supplier Duplicate Payments – 11.21/22		Advisory (significant weaknesses)	2 High priority actions	
<p>Through the use of data analytics, namely Alteryx software, we analysed an invoice paid transaction report covering the period February 2016 (Agresso inception date) to July 2021. The purpose of this was to identify potential duplicate supplier payments using five different tests.</p> <p>The transaction report included 240,793 payment transactions, which amounted to expenditure of £1,695,360,788 over the period. A total of 7,500 potential duplicate payments (9,978 transactions) were identified, valued at £13,175,192. We selected judgemental samples and investigated to ascertain whether there was a strong likelihood these were likely to be genuine duplicate payments. Investigations included reviewing monetary and supplier transactions on the Agresso system in order to determine whether there was evidence of corrections (credit notes, reversals or refunded amounts).</p> <p>Based on our investigations, we have identified a total of 33 payments (based on 66 individual transactions), valued at £194,467 where there is a strong likelihood duplicate payments have been made.</p> <p>We have not included the detail of the weaknesses due to the sensitive nature of this work, but this has been shared internally with relevant Council staff.</p>				
1	The Council will consider corroborating those payments identified in our investigations as having a strong likelihood of being duplicates (Appendix B) to confirm whether these are true duplicate payments. Where true duplicates are identified, suppliers will be contacted in order to provide repayment.	High	31 March 2022	Jasvinder Dalvair, Purchase to Pay Manager
2	Following the completion of the action above and using the Alteryx testing outcomes, the Council will extend investigations to identify other true duplicate payments that were not included in sample testing as part of this review. RSM may be commissioning to complete these further investigations or these could be undertaken internally.	High	31 May 2022	Jasvinder Dalvair, Purchase to Pay Manager

Temporary Accommodation – 21.21/22



7 High
7 Medium
3 Low



Housing Strategy and Homelessness Strategy

As part of the 2020/21 TA Review, we identified that the Housing Strategy (2016-2021) was currently in the process of being updated, with this taking place in consultation with external consultants Campbell Tickell. Throughout the audit, we were not provided with evidence to identify the progress made in relation to updating the Housing Strategy. We also identified through review of a transaction report relating to invoices received from Campbell Tickell that the most recent invoice was dated 15 December 2020, indicating the consulting work around the Housing Strategy may have ceased.

If a Housing Strategy and Homelessness Strategy are not in place and progress against objectives / actions are not monitored, there is an increased likelihood that organisational objectives may not be achieved. Furthermore, absence of a clear strategy, increases the likelihood that coordinated action is not taken to address issues. **(High)**



Resources

As per the latest TA snapshot report (dated 8 November 2021), a total of 433 households were housed in TA, with one Officer assigned 274 households and the other 159 (average of 217 households per Officer). This is a significant increase in terms of caseload for Officers when compared against the equivalent snapshot report dated 28 December 2020 where there was a total of 357 households, across three different TA Officers (an average of 117 households per Officer). This is also a disproportionate split between the two Officers.

The above indicates a significant resource gap, meaning there is a potential risk of insufficient staffing in place to allow the Council to deliver its statutory duties with regards to the Housing Act 1996 and Homelessness act 2002. Throughout the audit, we have noted a number of issues linked to the above resourcing issues identified. **(High)**



Analysis - Timeliness of Homelessness Decisions

We were advised by the Housing Demand Manager that there remain significant issues in relation to the timeliness with which homelessness decisions are made, with this largely owing to high levels of staff shortages. To substantiate this, we obtained a report from the Principal Performance and Quality Officer which noted that across 631 decisions made between April and November 2021, 386 (63.4 per cent) were outside the 56-day target.

If there is a delay in reaching a homelessness decision, there is an increased potential for ineligible households to remain in TA properties after the relief duty period of 56 days. There is therefore an increased likelihood that new applicants cannot be accommodated within the Council's TA property portfolio and the TA Team are forced to use nightly rate shared and bed and breakfast properties which incur higher nightly rate charges (impacting value for money). **(High)**



Rent Arrears Levels

We identified that as 31 October 2021, the Council had a total of £183,340 of TA current arrears outstanding against a target of £130,000 and £553,557 of TA arrears outstanding against a target of £295,000. When compared against data presented during our previous audit (dated January 2021), we can see that the current rent arrears position (both current and former) has increased from £142,983 and £467,769 respectively.

The Housing Recovery Lead advised that the increase in arrears levels mainly lies with the Council's inability to evict tenants between March 2020 and May 2021 (in light of the COVID-19 Pandemic), which has meant that arrears levels have continued to rise.

However, if sufficient action in relation to rent recovery for households in TA is not taken, there is a risk that the level of rent arrears will continue to rise. **(High)**



Safety Assurances from Private Providers

We identified a total of 16 private providers of accommodation to households within TA across 361 households. Following investigation, we identified that seven of these providers did not have an annual compliance statement (which notes the agreement of the provider to comply with the minimum safety requirements, including gas, electric and fire safety). Further, of the remaining nine providers, only one of these had been completed in the last year.

Without receiving assurances regarding the completion of safety checks for properties, the Council cannot be assured that properties used to meet TA needs are suitable in terms of safety. **(High)**



Analysis – TA Households

We analysed the latest TA Snapshot report (dated 8 November 2021) and identified a total of 466 Homeless Applications. We analysed the date the homeless application had been completed by the above mentioned 466 and found that 37 per cent of applicants have spent more than three years in TA, with one applicant having made their application in December 2012. More information can be found within the detailed findings.

This highlights that the Council are not efficiently moving households out of TA. This was supported through discussions with both the Housing Demand Manager and the Group Manager – Accommodation, who advised that the Council currently does not have a strategy in place to progress households out of TA. In absence of a clear strategy, there is a risk that numbers of households in temporary accommodation continue to rise, expending Council resources and increasing the TA Team's reliance on the use of public-sector rented accommodation. **(High)**



Council Owned Buildings – Safety Assurances

We were advised by the Housing Demand Manager that monthly returns to the Corporate Building Compliance Group are made, detailing safety compliance performance data across Council owned stock, including TA. However, at the date of review, we were not provided with evidence to substantiate this. If the safety compliance is not effectively monitored with regards to Council-owned TA, there is a risk that safety compliance gaps are not identified and rectified in a timely manner. Therefore, if properties are not safe, there is an increased risk of reputational damage where households are placed in unsuitable accommodation. **(High)**



Reporting

We noted through discussion with the Housing Demand Manager that since the restructure, there have only been one meeting of the Community – Accommodation and Neighbour Management service line (dated 6 October 2021) where the group’s purpose was discussed (rather than Housing related KPIs, including TA).

We did identify that whilst these meetings are not taking place, monthly performance reporting had been sent to attendees of the meetings in August, September and October 2021. Across the three sampled months, we identified performance with respect to each KPI had been declining (see table above). This was also true when compared to performance data identified as part of the 2020/21 Internal Audit review.

We also noted that comments/ supporting narrative to explain the performance had not been noted within the report, nor had any remedial actions to address these issues had been documented.

In absence of monthly monitoring of KPI indicators in relation to Community - Accommodation and Neighbourhood, there is a risk that service level issues are not identified, investigated and rectified in a timely manner. **(Medium)**



Periodic TA Audits

Once the Council has a duty to accommodate persons who are not intentionally homeless (S193) and they have been accommodated, the TA Officer contact the tenant six weeks, three months and one year after, with the details of call captured on TA audit form. Through discussion with a TA Officer, we were advised that periodic TA audits are currently not being consistently completed, with this largely owing to prioritisation of other work in light of resource constraints within the team (see above).

If TA visits are not undertaken in a timely manner, or not undertaken at all, there is an increased likelihood that tenant problems and concerns may go unresolved for some time, thus negatively impacting the reputation of the Council. Furthermore, if reasons for untimely visits are not documented, the TA team cannot identify the underlying causes for delays, limiting the ability to adequately monitor the completion of household visits. **(Medium)**



Allocations

When an individual informs the Council that they are at risk of homelessness, the Housing Demand Team will undertake an initial assessment to determine whether the Council holds an interim duty to accommodate. Once a decision is made by the Team, the TA team is notified who is then responsible for identifying appropriate accommodation.

Whilst we requested evidence to substantiate whether the above processes had been appropriately followed for a sample of 20 households, at the date of review, none of the requested evidence had been provided. The Council are therefore unable to take assurance in relation to processes that are in place to identify and allocate housing based on need and available options as well as the agreement of licenses for TA and the completeness of these documents retained. **(Medium)**



Homelessness Decisions (Positive)

Once the Housing Demand Team have made their assessment (and the outcome is 'positive'), the TA Team are responsible for completing an assessment of current accommodation to ensure that these household are accommodated in line with the Council's Placement Policy. We selected a sample of 10 'positive' decisions made in the 2021/22 financial year, however, were not provided with evidence to confirm that such a reassessment of accommodation has taken place.

If a reassessment of the suitability of existing TA are not taking place, there is a risk that homeless individuals are inappropriately placed. **(Medium)**



Negative Decisions (Negative)

Once the Housing Demand Team have made their assessment (and the outcome is 'negative', the TA Team are responsible for issuing a notice to quite to evict the household from their TA. We selected a sample of 10 'negative' decisions made in the 2021/22 financial year, however, were not provided with evidence to confirm that a notice to quite had been issued and that the property had been vacated in a timely manner.

Should households who had received a negative decision not receive a notice to quit in a timely manner, there is a risk that the Council will suffer financial losses where rent arrears are increasing in these properties whilst they are not being vacated. **(Medium)**



Breach of License

We requested a report/listing of cases where a notice to quit had been issued in the current financial year, however this was not received. As such, we were unable to select a sample to complete substantive testing to confirm that due protocols are consistently taken once a household is in breach of their license agreement.

If consistent/ appropriate processes are not taken following breaches of licenses, this may result in repeat offences as well as delays in evicting such licensees. **(Medium)**



Analysis – Private Sector Providers

Through discussion with the Housing Demand Manager, we identified that the Paradigm Housing Association (the Council's largest provider) had notified the council that they were ceasing operating in the next financial year. Our analysis identified that Paradigm accounted for 23 per cent of all private rent accommodation (more than double of each provider, with the exception of Ashburn Properties) therefore meaning that these households would need to be rehomed, at significant disruption to the licensees as well as the Council's resources.

The Housing Demand Manager advised that the Council has not agreed, nor considered a strategic approach to utilising private rented accommodation, including standards by which the Council can diversify their portfolio of accommodation.

Failure to effectively diversify the Council's portfolio of private rented accommodation increases the risk of significant disruptions to Council resources should a provider collapse. This could also lead to reputational damage to the Council where households are required to move. **(Medium)**

1	In line with current plans, the Council will ensure that an up-to-date Housing Strategy and Homelessness Strategy is created. Additionally, progress against the action plan will be periodically monitored by an appropriate forum.	High	30 September 2022	Dean Tyler - Associate Director – Place Strategy and Infrastructure
2	The Council will undertake a review of workload for Officers and if deemed appropriate, create a business case to add additional resource in this area to aid the Council in meeting their Statutory responsibilities in respect of Temporary Accommodation.	High	30 September 2023	Ian Blake – Group Manager – Accommodation
3	Following completion of the corporate restructure, a new performance mechanism will be developed to reflect the new service. This will include periodic consideration of Temporary Accommodation related performance indicators.	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation
4	The Temporary Accommodation Team will design interim measures to ensure that tenants are interacted with through periodic calls to identify any issues with their accommodation (or other related matters).	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation
5	The Temporary Accommodation Team will ensure that all documentation relating to the TA allocation (including spot placements) processes are retained via DIP.	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation
6	The Council will undertake a review of workload for Officers and if deemed appropriate, create a business case to increase capacity in this area to help the Council in meeting their Statutory responsibilities, in respect of Housing Decisions. Following this, the timeliness of decisions will be monitored through monthly performance reporting (as per management action five).	High	30 September 2023	Ian Blake – Group Manager - Accommodation
7	The Temporary Accommodation Team will ensure that following notification from the Housing Demand Team, a reassessment of accommodation is completed to ensure that this is suitable and in line with the Team’s Placement Policy.	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation
8	The Temporary Accommodation Team will ensure that following notifications are received from the Housing Team: <ul style="list-style-type: none"> • The negative decision has been recorded on Capita; • A notice-to-quit has been issued; 	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation

	Assurance is received to ensure that the accommodation had been vacated by the previous licensee.			
9	The Temporary Accommodation Team will ensure notices to Quit are served where the tenant breaches the licence agreement with the Council, with this in line with Council Policy.	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation
10	The Council will take action to improve the Council's rent arrears profile for those housed in Temporary Accommodation. Collection rates will be reviewed via KPI reporting as per management action five.	High	30 September 2023	Ian Blake – Group Manager - Accommodation
11	The Annual Compliance Statement issued to Private Providers will be reviewed to assess whether the terms and conditions satisfies the Council's legislative duties as a housing provider. Following this, the Council will introduce a monitoring mechanism to ensure: <ul style="list-style-type: none"> Providers are only engaged with should they have a signed Compliance Statement in place; These Compliance Statements are reviewed and signed annually. 	High	30 September 2022	Ian Blake – Group Manager - Accommodation
12	The Temporary Accommodation Team will ensure that monthly safety compliance of Council-owned stock (relating to properties in TA) are monitored on a monthly basis.	High	31 December 2022	Ian Blake – Group Manager - Accommodation
13	The Council will develop a strategy to identify households which are no longer owed a duty to be accommodated under the Housing Act 1996.	High	31 March 2023	Ian Blake – Group Manager - Accommodation
14	The Council will develop a diversification strategy to engaging with private rented accommodation providers.	Medium	31 March 2023	Ian Blake – Group Manager - Accommodation

Risk Management – 19.21/22		2 High 6 Medium 3 Low
-----------------------------------	---	--



Assurances against risks / controls

We noted through review of the Corporate Risk Register that assurances in relation to the effectiveness of controls in place are not currently documented (as at December 2021). This was identified in our previous Risk Management review and although the action was marked as 'implemented' and closed within the Council's action tracking software, it has not been implemented. While the Council receives third line assurance from Internal Audit through a risk based audit plan, and potentially from a range of other third line (independent) assurance providers (e.g. Ofsted, the CQC, the DLUHC, CIPFA, Information Commissioner etc) without the Risk Register documenting the assurances received against controls designed to mitigate risks, there is an increased chance of risks being realised (if controls are not operating as intended). Independent assurances can be effectively used to inform where further action may be required. **(High)**



Directorate Risk Registers

As part of the 2020/21 Risk Management review, a medium priority management action was agreed in relation to the following:

"On a monthly basis, the Senior Risk and Insurance Officer will review each of the directorate risk registers and highlight any exceptions. These exceptions will be communicated to the relevant members of the respective DMT, with remedial action taken as appropriate. The actions will be followed up on monthly and where inadequate progress has been made, this will be escalated as appropriate."

Through discussion with the Risk and Insurance Officer, we were informed that they had not been invited to all directorate meetings to discuss and review the risk registers. Subsequently the post holder left their role with the Council with the Group Manager (Commercial), picking up risk management responsibilities in the interim. We noted through review of Risk and Audit Board meetings for the 2021 calendar year, that directorate risk registers had not been regularly reviewed, part of which could be attributed to staff turnover and changes in the directorates and the Risk and Insurance Officer leaving the Council.

At the time of audit, the Council only had a Corporate Risk Register in place, and while a revised directorate structure was in place, in the absence of directorate risk registers, it was not clear how strategic and operational risks were being identified, documented, discussed and managed, increasing the chances of risks being realised within directorates, which may have an impact on the Council's ability to achieve their objectives/outcomes. **(High)**



Risk Management Training

Following the restructure, the Council's Risk and Insurance Officer left the organisation, with the risk management arrangements being led by the Group Manager - Commercial, and the Director of Finance, predominantly through the Risk Board.

An action was agreed in our 2020/21 audit to introduce risk management training, however as at November 2021, formal risk management training had not been rolled out. An options appraisal for conducting training was presented to the Risk and Audit Board in September 2021, and "the board agreed that the option to roll out online training through cornerstone would be the most effective option for the Council at this point".

However, at the time of audit this had not been rolled out to either staff or members. If relevant risk management training is not provided, there is a risk that risks may not be identified, documented and effectively and consistently managed. This increases the likelihood that risks may materialise. **(Medium)**

Following the audit, we were informed that Risk Management Training had been set up and was being delivered, however we have not reviewed the content of the training or that the Council have set compliance targets with regards to completion, and this will be tested as part of the 2022/23 Risk Management Audit.



Risk Management Strategy

We were provided with the Risk Management Strategy and confirmed through review of the document that whilst it had been updated to include a statement on the Council's risk appetite which was part of the action agreed in the 2020/21 Risk Management report, this was still inconsistent within the document and had not been amended following actions agreed in the previous report (referred to above).

We noted that while the version history section of the document stated that the strategy had been approved by the Audit and Corporate Governance Committee in June 2019, review of all minutes of the Audit and Corporate Governance Committee for both 2019 through to 2021 found no reference to the Risk Management Strategy being presented for approval, and it was last approved in December 2018.

We confirmed through review of the Audit and Corporate Governance Committee's Terms of Reference (ToR - held within the 2021 Constitution on the Council's Internet page) that the requirement to approve the Risk Management Strategy had been included, however we could not find evidence to confirm this had been done since December 2018.

Failure to clearly document the Council's risk management strategy and receive formal approval of the strategy may result in inconsistent practices in relation to risk management being adopted across the Council. **(Medium)**



Corporate Risk Register Content

We reviewed all 15 risks documented within the Corporate Risk Register and reviewed the risk scores to ensure they were consistent with the strategy and the wording of the risks, controls and actions required.

While we noted that each risk was owned by either the Executive Board or an individual Director, responsibilities for implementing the actions identified (which may be separate to the risk owners as the risks have been assigned at a strategic level) or dates for implementation were not consistently assigned for each of the actions.

While we appreciate that the revisions to the Risk Register are a work in progress, following the restructure and changes in the responsibilities for risk management, without consistently documenting the timescales and owners for actions to improve the control framework increases the risk of actions not being implemented and may contribute to risks being realised. It also reduces the visibility to readers of the risk register how and when actions will be completed. **(Medium)**



Links to Strategic Objectives

We reviewed the latest version of the Corporate Risk Register and while we noted that a total of 15 risks had been included, none of the risks documented were aligned to strategic objectives.

We were informed that the Council's five year plan is no longer in use, and a recovery plan is being developed as the council's key strategic plan. The Council will need to ensure that the Corporate Risk Register aligns to the outcomes in the Council's recovery plan in order to take assurance that it has identified all of the risks in relation to achieving its outcomes/objectives.

We noted that while some of the risks on the register are of strategic importance following the issue of a S114 notice and the restructure and subsequent reports from MHCLG (now DLUHC) and CIPFA, these risks can be seen as cross-cutting all of the Outcomes, and without documenting the relevant outcomes in the Corporate Risk Register and aligning these to the risks identified, it is difficult to conclude that the Council has identified all relevant strategic risks or that all of the risks documented are actually strategic risks. This could increase the risk of outcomes not being achieved if the Council is not aware of all relevant strategic risks. **(Medium)**



Cabinet reporting

We reviewed the agendas and papers for Cabinet meetings held since March 2021 and could not find evidence to show that, in line with the Risk Management Strategy, the Corporate Risk Register had been provided to Cabinet, or that the Cabinet had reviewed "the Council's approach to Risk Management and approve changes or improvements to key elements of its processes and procedures".

We also could not confirm that the Cabinet had set the Council's risk appetite in line with the Risk Management Strategy, nor whether the Cabinet "periodically reviewed the Council's approach to Risk Management" or how Cabinet had determined whether the Council was "risk taking or risk averse", as coverage of these areas were not in the minutes or papers provided to Cabinet. Following the review, we were informed that the role of the Audit and Corporate Governance committee and how it reports to Cabinet is being determined, as this could form part of the annual report from the committee to Cabinet.

There is a risk of poor governance if the Council does not operate risk management in line with the current strategy in place, which could lead to risks not being effectively managed or allowing the opportunity to take appropriate mitigating action. **(Medium)**



Risk and Audit Board

We noted that from July 2021, the Risk and Audit Board was reformed and the ToR reviewed, however we found that the attendance requirements for Associate Directors was not always being complied with.

We also noted that the Board was not consistently fulfilling its responsibilities, for example in terms of scrutinising previously agreed internal audit management actions, and receiving updates in relation to Business Continuity. There is a risk of insufficient scrutiny by the Risk and Audit Board which could lead to risks being realised. **(Medium)**

1	<p>The Risk Management Strategy document format will be updated to include a next review date and the contents of the strategy will be updated to include:</p> <ul style="list-style-type: none"> the requirement for identified risks to be linked to strategic objectives; the current responsibilities of cabinet; the responsibilities of members of DMT meetings to scrutinise the content of risk registers 	Medium	1 August 2022	Clare Priest – Group Manager, Commercial
---	--	--------	---------------	--

	<ul style="list-style-type: none"> the responsibility of Directors to monitor the progress of overdue directorate level risk management actions. <p>Subsequently, the Policy will be communicated to all staff and approved by the Audit and Corporate Governance Committee on an annual basis.</p>			
2	The Corporate Risk Register will be updated so that all actions identified consistently have owners and implementation dates recorded.	Medium	30 September 2022	Clare Priest – Group Manager, Commercial
3	The Council will roll out risk management training and maintain a central log to show which staff have been training. In addition, the Council will develop a training matrix to identify and prioritise those staff with risk management responsibilities.	Medium	31 March 2022 / Complete	Clare Priest – Group Manager, Commercial
4	The Council will align each of the risks within the Corporate Risk Register to the outcomes of the Council's recovery plan.	Medium	30 September 2022	Clare Priest – Group Manager, Commercial
5	Risk Owners, as part of the review of the Corporate Risk Register, will review assurances against the controls in place, scrutinising the source and strength of that assurance. Where the assurances either indicate issues, or where there are a lack of assurances against controls, action will be taken to address these, and the residual risk scores for risks will be updated accordingly.	High	30 September 2022	Corporate Leadership Team
6	The ACG will report into Cabinet in line with the Audit and Corporate Governance Committee Terms of Reference paragraph 35 article 9	Medium	Complete	Angela Wakefield – Monitoring Officer
7	The Risk and Audit Board will ensure: <ul style="list-style-type: none"> Attendance is in line with the Terms of Reference (specifically Associate Directors) For all Internal Audit actions, the Risk and Audit Board should seek assurance from the GM - Commercial that sufficient evidence has been reviewed to confirm that the actions have been implemented before being closed. <p>Appropriate business continuity updates are provided which clearly link to issues identified as part of Internal Audit reviews.</p>	Medium	30 June 2022	Clare Priest – Group Manager, Commercial



8	Risk Registers will be formulated for each of the directorates and a revised schedule for the review of Directorate Risk Registers will be agreed by the Risk and Audit Board.	High	30 June 2022	Clare Priest – Group Manager, Commercial
---	--	------	--------------	--

<p>Capital Expenditure – 23.21/22</p>		<p>2 High 7 Medium 3 Low</p>
<p>Business Case Preparation and Approval</p> <p> Business cases are prepared for capital bids, with scrutiny and approval required before being added onto the capital programme. For a sample of ten capital projects included within the programme as at September 2021, we identified that six business cases had not been internally signed off (as completed), with business cases not provided to us for another three of the sample. Evidence of business case approvals were also not provided for seven of the projects. Although the procedure for business cases was under review at the time of our audit, where business cases are not adequately prepared and approved there is a risk projects are added to the capital programme without (or with inappropriate) authorisation. (High)</p> <p>Project Monitoring and Reporting</p> <p> There is no consistent approach for monitoring and reporting all capital programme projects, with portfolio projects not reported upon since September 2021 and non-portfolio projects no longer being reviewed once completed. Part of this may be attributed to the restructure, which removed the Project Management Office (PMO) from the structure. For our sample of ten projects, we requested evidence of monitoring and reporting, however this was not provided. Without an agreed formal approach for monitoring and reporting all capital projects, there is a risk staff/Members are not informed of progress and that issues are not identified and resolved in a timely manner. (High)</p> <p>Financial Procedure Rules</p> <p> The Council’s Financial Procedure Rules (FPRs) include high-level information relating to capital expenditure processes. Through review, we found that despite the contents covering the capital strategy, budget, projects and responsibilities, there were a number of inconsistencies with current practice (including job roles, forums and directorates) and limited information on other processes such as carrying funds forward. The FPRs were due to be updated and presented for approval in January 2022, however this did not occur and instead a revised intention was stated that they would be prepared and adopted from April 2022. If the FPRs do not provide clear and accurate information, there is a risk that readers have insufficient guidance with regards to capital expenditure processes. (Medium)</p>		



Capital Guidance (including capital expenditure)

Although not available at the beginning of our audit, guidance relating to capital expenditure was prepared over the course of our fieldwork testing. Through review, we noted that this guidance focussed solely on the capitalisation of expenditure, with no information on other capital processes such as preparing bids and monitoring projects. Through discussions as part of our review and our audit findings we identified that many of the expectations and processes related to capital expenditure were unclear or unknown to staff. Without suitable guidance materials, there is a risk that capital processes are completed incorrectly, impacting the delivery of the programme. **(Medium)**

Carry Forward



Earmarked Reserve forms were completed in previous years where services wished to carry forward capital funds, however this process was undergoing review at the time of our audit due to historical issues with limited scrutiny and blanket approvals being granted as part of budget approval. The process for carrying forward capital funds should consider why amounts were not spent and the funding source, as well as ensuring requests are subject to suitable scrutiny. Without this, inappropriately carried forward amounts may be included in the capital budget, impacting opening balances and the accuracy of financial statements. **(Medium)**

In-Year Changes



There is a lack of clarity with regards to how in-year changes to the capital programme should be proposed and agreed, with a contrast between the Financial Procedure Rules and historical practice. A report brought to Cabinet in July 2021 stated there had been a failure to comply with capital spend approval, including in-year changes such as additions. Although this process was being reviewed and agreed at the time of our audit, without a robust procedure there is a risk inappropriate changes to the programme are implemented. This may impact the allocation of capital funds, delivery of projects and Council finances. **(Medium)**

Capitalised Expenditure



Expenses associated with capital projects are funded via the capital programme, with capitalised expenditure assigned a 'P' code on Agresso. Investigations following the 2018/19 external audit have highlighted significant issues with the incorrect capitalisation of revenue expenditure. At the time of our review, we confirmed that the Council had implemented interim controls to detect transactions that were incorrectly capitalised, such as the capital accountants reviewing transaction lists. However, without permanent, robust controls in this regard, there is a risk that costs will continue to be incorrectly capitalised, inflating the cost of assets which may result in financial misstatement. **(Medium)**

Internal Capital Governance



The Capital Monitoring Group (CMG) has not meet since December 2020, with its responsibilities being assumed by the Strategic Finance Board (SFB). Through review of SFB minutes ranging from May to October 2021 we found that whilst the capital programme was included as an agenda item at the meetings in May, June and July, this had not occurred at the most recent meetings (August and October). Although the capital programme was undergoing review over this time (and at the time of our audit). Without ensuring the capital programme is internally reviewed and discussed, there is a risk progress updates are not subject to suitable scrutiny. **(Medium)**



Combining the capital and procurement business cases

As part of the Capital Expenditure 2020/21 review, a management action was agreed to combine the capital and procurement business cases (into one document) and instruct staff to use this. We identified that whilst a combined business case for revenue expenditure had been prepared (although it was stated that this was also to be used for capital), this had not been finalised, approved for use, shared with staff or made accessible via the intranet. As such there remains a risk that without involvement of procurement, sufficient value for money may not be obtained for capital projects.

(Medium)

1	As part of the FPRs review, the Council will ensure that references, processes and expectations relating to capital expenditure are updated. This will include providing clarity where required.	Medium	31 July 2022	Alison Rogers – Financial advisor
2	Comprehensive procedure guidance will be prepared covering all capital expenditure processes, ranging from capital projects to financial functions. Guidance will align to the revised processes as per the Financial Procedure Rules and be shared with relevant staff, as well as being made accessible via the intranet.	Medium	31 December 2022	Brian Khumalo – Finance Business Partner
3	The Council will agree its approach for carrying forward capital funds where these are not spent in the assigned year.	Medium	30 June 2022	Brian Khumalo – Finance Business Partner
4	The Council will agree an approach for proposing, reviewing and approving in-year changes to the capital programme. This will include the requirement for changes to first be scrutinised and approved prior to being implemented.	Medium	31 December 2022	Brian Khumalo – Finance Business Partner
5	The Council will implement permanent controls to prevent and detect the incorrect capitalisation of expenditure.	Medium	30 September 2022	Brian Khumalo – Finance Business Partner
6	The Council will agree the arrangements for approving business cases and adding projects to the capital programme. This will include defined approval thresholds (based on project cost), escalation procedures (to ensure oversight of approvals/additions) and clarity regarding the evidence to be provided before projects are formally added onto the programme.	High	30 September 2022	Brian Khumalo – Finance Business Partner
7	The capital business case template will be prepared to incorporate procurement questions/requirements (as were previously included within the separate procurement business case).	Medium	30 June 2022	Clare Priest – Group Manager Commercial

	Once prepared, the template will be made accessible to all staff and a reminder email issued advising staff of the requirement to use this going forward.			
8	Monitoring and reporting arrangements for all capital projects included on the capital programme will be agreed and adhered to. These arrangements will cover 'on' and 'off portfolio' projects and will include ensuring progress updates are received.	High	30 September 2022	Brian Khumalo – Finance Business Partner
9	There will be a standing agenda item at Finance Board meetings for capital monitoring/capital programme. This will be used to discharge the duties and responsibilities as defined within the updated terms of reference.	Medium	Action complete – following the establishment of the Finance board which has replaced SFB	NA

<p>General Data Protection Regulation (GDPR) Governance – 24.21/22</p>	<p>Advisory (significant weaknesses)</p>	<p>3 High 12 Medium 1 Low</p>
<p> GDPR Action Plan Through review of the Information Governance Board (IGB) Action Trackers (used to also track GDPR actions) for July, September and October 2021, we noted that whilst all actions had an owner and status assigned, there was no due date recorded for any actions. We also noted that updates against actions were not being dated, and actions were not being regularly updated. Without effective tracking of actions, this could lead to outstanding areas of GDPR not being implemented in a timely manner. (High)</p> <p> Data Flow Mapping Through review of the Data Flow Capture spreadsheet, we noted that various fields had not been detailed, such as the 'GDPR Article 6 lawful basis for processing'. We also noted that the spreadsheet was not fully complete, for instance, fields had been left blank in the 'Detail the Business Purpose of Data Transfer' and 'Systems Data Classification' columns. If data is not appropriately mapped across the organisation, there is a risk of the organisation being unaware of the data being held, how such data is used by different departments and how it flows through the organisation. This could also lead to issues with lawfulness of processing, security and retention. (High)</p>		



Password Management

Through review of the IT Password Policy, we noted that it did not cover areas such as account lockout requirements or security monitoring to detect and alert the organisation to what may be indicators of malicious or abnormal behaviours. We also found that the actual Active Directory configuration was inconsistent with the Policy, as password expiry had been set to 180 days as opposed to the 90 days set out within the Policy.

Without a password policy that details all minimum requirements, and without adherence to this policy, there is a risk that inappropriate password settings are in place that do not adequately protect the organisation's systems against unauthorised access. **(Medium)**

Records Management

Through review of the Information and Records Management Policy, we noted that it was due for review in May 2019 and was therefore out of date. In terms of content, we noted that the Policy did not provide detailed information on managing the security of records or disciplinary information for breach of the policy.



We also found that the Policy referenced a Records Disposal Schedule and what it should cover, however, this did not align to the Corporate Retention Schedule actually in place, for instance, the Records Disposal Schedule referenced storage arrangements whereas the Corporate Retention Schedule did not.

Through review of the Corporate Retention Schedule, we noted that it was due for review in April 2019 and therefore required updating. We also noted that it did not cover areas such as format of the record or the retention trigger. Furthermore, we noted that the Schedule was not fully complete. Without a comprehensive policy and schedule in place, this could lead to an inconsistent approach to data storage and retention, potentially leading to personal data being mismanaged. **(Medium)**

Management Awareness



Through review of the IGB minutes for July, September and October 2021, we noted that data breaches were included as a standing agenda item in all cases and discussed. We noted however that other areas of GDPR, such as compliance with GDPR training or personal data requests, were not being discussed. This increases the risk of a lack of oversight of data protection requirements, resulting in data issues existing that may lead to legislative non-compliance and control weaknesses. **(Medium)**



Data Protection Policy

Through review of the Data Protection and Privacy Policy, we noted that it had not been updated since May 2018, despite requiring annual review. In terms of content, we also noted certain information was not included, such as the lawful bases for processing information. Without a comprehensive and up to date policy, this could lead to an inconsistent approach to data protection or staff being unaware of key areas, potentially leading to personal data being mismanaged. **(Medium)**



Privacy Notice

We found that the Privacy Notice was not easily accessible on the Council's website, as the 'Privacy' link on the home page did not correspond with the full Privacy Notice and only provided some brief information on privacy. On review of the content of the Privacy Notice, we noted certain areas were not covered, such as the right to lodge a complaint with a supervisory authority. Without a comprehensive and easily accessible privacy notice, this could lead to data subjects not being aware of all information required to comply with their right to be informed about their personal information. **(Medium)**

Personal Data Requests

We were advised by the Acting Data Protection Officer (DPO) that a procedure had not yet been developed to detail how the organisation will deal with data subjects exercising their rights, such as the right to rectification, data portability and erasure. This could result in an inconsistent approach by staff to dealing with personal data requests, potentially leading to rights not being met appropriately or in a timely manner. **(Medium)**



Through review of the Subject Access Requests (SARS) Log, we noted that it did not cover certain areas such as whether the identity of the data subject (or third party) has been verified. We also found that requests were not being consistently complied with within one calendar month (of the 58 closed requests, eight were late, ranging between one day and one month late). This could lead to data subjects not being aware of all information in a timely manner in order to manage their personal information appropriately.

Through review of the SBC Right to Removal Log, we noted that it was not in a consistent format with the SARS Log and was also missing certain areas, such as whether the request has been made by a third party on behalf of a data subject. This could lead to key information with respect to Personal Data Requests not being retained for analysis and investigation where required. **(High)**

Lawful Bases



Through discussion with the Acting DPO, we were advised that although the Council is aware of the lawful bases it uses to process personal information (such as contract), this had not been formally and centrally documented and agreed. If the lawful bases identified by the organisation are not documented, there is a risk that staff will be unaware of the lawful bases in which personal data is obtained, or lawful bases being inconsistently applied. **(Medium)**

Consent



We were advised by the Acting DPO that the Council did not have a policy/procedure in place for the management of consent under GDPR. If the processes for obtaining consent are not appropriately documented, there is a risk that staff will be unaware of the requirements to adhere to under GDPR to obtain consent from data subjects. **(Medium)**

Despite numerous requests, we were not provided with any template forms being utilised by the Council to capture consent under GDPR for the processing of personal data. Without appropriate forms, this could lead to the Council not informing data subjects of key information prior to obtaining their consent to process their personal data. **(Medium)**

Data Breaches



Through review of the Information Security Incident Reporting Policy, we noted that it had last been reviewed in May 2018, despite requiring annual review. In terms of content, we found certain areas not covered, such as timescales for reporting a data breach to the ICO. Without a comprehensive policy, this can lead to data breaches not being effectively and consistently managed by staff to ensure damage is minimised and further breaches are prevented. **(Medium)**

Through review of the Data Breach Log, we noted that near misses were not being recorded in addition to breaches. Moreover, further information was not being recorded, such as format of the data lost/impacted or whether the breach was notifiable to the ICO. This could lead to key data breach information not being retained to ensure sufficient audit trail and to inform thematic analysis of breaches to identify trends to be addressed. **(Medium)**



Third Parties

Despite numerous requests, we were not provided with information relating to the management of third parties with respect to GDPR (although the DPO advised that this was being managed by another department). We have therefore not carried out any further testing in this respect. Without a

third-party register, this could lead to ineffective tracking of third parties, resulting in personal data being shared without appropriate safeguards. Moreover, without appropriate templates in place, this could result in personal data being shared with third parties without appropriate safeguards. **(Medium)**

1	The Information Governance Board Action Tracker will be updated to include due dates for all actions. Following this, dated updates will be recorded against all overdue actions at each meeting.	High	30 April 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
2	<p>The Data Flow Capture Spreadsheet will be updated to include the following areas:</p> <ul style="list-style-type: none"> • name and contact details of joint controller (if applicable); • categories of individuals; • names of third countries or international organisations that personal data are transferred to (if applicable); • safeguards for exceptional transfers of personal data to third countries or international organisations (if applicable); • Data Protection Act 2018 Schedule 1 Condition for processing; • GDPR Article 6 lawful basis for processing; • link to retention and erasure policy document; and • whether personal data retained and erased in accordance with the retention policy document - reasons for not adhering to retention policy document (if applicable). 	High	30 September 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
3	<p>The Council will update the IT Password Policy to include:</p> <ul style="list-style-type: none"> • account lockout requirements (number of attempts (threshold), lockout duration and counter reset time) • where and how staff may record passwords to store and retrieve them securely; • if password management software is allowed, and if so, which; • which passwords staff really must memorise and not record anywhere; • password configuration for administrators; • dealing with the configuration of passwords within software/applications, such as firewalls and social media; • security monitoring to detect and alert the organisation to what may be indicators of malicious or abnormal behaviours, such as: login attempts that fail the second step of Multi Factor Authentication and brute forcing of account passwords; • the use of password deny lists or a process to reactively search a password database for the hashes of deny list passwords (and using this to inform training); and • disciplinary with respect to non-compliance with policy. 	Medium	31 May 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)

	Following this, the Council will ensure that the password configuration in practice matches the updated Policy and that the revised Policy is circulated to staff.			
4	<p>The Information and Records Management Policy will be reviewed and updated to include details on managing the security of records and disciplinary information.</p> <p>In addition, the Corporate Retention Schedule will be updated to include:</p> <ul style="list-style-type: none"> • format of the record (electronic, paper etc.); • storage location; • record owner; • retention trigger; • action at the end of retention period (review for further retention, anonymise, destroy etc.); and • method of disposal. <p>Following this, the Schedule will be fully completed and referenced in the Information and Records Management Policy accordingly.</p>	Medium	30 September 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
5	<p>The Council will discuss the following as part of Information Governance Board meetings, with this being reflected in the Terms of Reference:</p> <ul style="list-style-type: none"> • GDPR training compliance; • compliance with personal data requests under GDPR; and • any other (GDPR) business. <p>Further thought also needs to be given to where the IGB reports / escalates issues to (ie Risk and Audit Board etc).</p>	Medium	30 April 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
6	<p>The Data Protection and Privacy Policy will be updated to cover:</p> <ul style="list-style-type: none"> • lawful bases for processing information (including additional conditions for special category data); • potential fines for non-compliance with GDPR in the event of a data breach; • the right of individuals to claim compensation for damages caused by a breach; • GDPR rights (including circumstances where they apply etc.) • dealing with transfers of data outside of the EEA; • disciplinary information for breach of the policy; • key data protection definitions/terminology; and • contact details of the DPO. <p>Following review, the policy will be communicated to all staff.</p>	Medium	30 June 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)

7	<p>The Privacy Notice will be updated to cover:</p> <ul style="list-style-type: none"> • the right to object; • rights in relation to automated decision making and profiling; • the right to lodge a complaint with a supervisory authority; • the details of whether individuals are under a statutory or contractual obligation to provide the personal data; and • the details of the existence of automated decision-making, including profiling. <p>Following this, the Council will review the location of the Privacy Notice on its website to ensure it is easily accessible from the home page.</p>	Medium	31 May 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
8	<p>A procedure will be produced to detail how the Council will deal with individuals exercising each of their rights under GDPR such as the right to rectification, data portability and erasure. This will cover areas such as:</p> <ul style="list-style-type: none"> • how requests can be made (verbally, email, letter etc.); • the rights of individuals under GDPR (and therefore the types of requests that can be made); • responsibilities of key staff; • definitions (such as data subject, personal data, lawful basis etc.); • when the rights apply (as some are scenario specific); • verifying the identity of data subjects making a request (including third parties acting on behalf of data subjects); • establishing authority of a third party making a request on behalf of a data subject; • charging fees; • what information to provide the individual in addition to the data requested, in line with ICO guidance; • circumstances for refusing to act on a request; • what information to provide the data subject if a request is refused (i.e. the reason for refusal, how to make a complaint to the ICO or how to seek judicial remedy etc.); • response times and formats (such as hard copy, email, orally etc.); • what to do if there is going to be a breach of timescales for responding to the request; • circumstances when the response time can be extended; • logging of requests and retention of data received/retrieved/recorded (in case the data is challenged by the data subject); • how each data subject right is to be dealt with; • dealing with data that includes information about other individuals (for instance, a HR file which contains information identifying managers and colleagues); • dealing with requests where the organisation needs to amend the data before sending out the response; • dealing with requests for children's data (if applicable); 	Medium	31 May 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)

	<ul style="list-style-type: none"> • dealing with complaints/appeals; • dealing with exemptions; • details on enforced SARs; and • response letter templates. 			
9	<p>The SARS Log will be updated to include:</p> <ul style="list-style-type: none"> • date request received (at the moment, only the 'Date Reported' is recorded); • staff member who received the request; • format of the request received; • description of the request; • whether the identity of the data subject (or third party) has been verified; • whether the request has been declined; • if declined, why the request has been declined; • if declined, when the data subject was informed of this; • whether the request has been made by a third party on behalf of a data subject; • if the request has been made by a third party, whether the authority of the third party has been established; • if the request has been made by a third party, whether the identity of the third party has been established; • the staff in the organisation that the information has been requested from; • date information requested from staff; • date information received from staff; • what information has been sent to data subject; • in what format the information has been sent to the data subject; • date request is due; • whether there has been an extension to the deadline; • if there has been an extension, when the data subject was informed; and • whether the information was sent to the data subject within the required deadlines. <p>Once updated, the Council will ensure that the SBC Right to Removal Log for other personal data requests is consistent with the updated template.</p> <p>Following this, the Council will ensure that all requests are complied with in line with the ICO deadlines.</p>	High	30 June 2022	Finbar McSweeney Complaints, Casework & FOI Lead
10	<p>The Council will formally document and agree the lawful bases for the different types of data processed by the organisation. This will include the rationale for the lawful bases as relevant. Subsequently, this will be communicated to relevant staff.</p>	Medium	30 June 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)

11	<p>A Consent Policy/Procedure will be documented, approved and communicated to all staff. This will cover areas such as:</p> <ul style="list-style-type: none"> • how to consider whether consent is the most appropriate lawful basis for processing; • how a consent request should be written; • what information a consent request should detail (including reference to the relevant Privacy Notice); • what methods can be used to indicate consent; • how consent should be recorded; • how consent should be managed and refreshed where relevant; • how to manage the right to withdraw consent; • how to identify and verify the age of data subjects to ensure that parental consent is obtained where required; and • template consent forms. 	Medium	30 June 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
12	<p>The Council will ensure that all forms used to capture consent under GDPR cover:</p> <ul style="list-style-type: none"> • the name of the organisation/any third-party controllers who will rely on the consent; • a copy of the privacy notice or reference to this and where it is available; • why the organisation wants the data (the purposes of the processing); • what the organisation will do with the data (the processing activities); • whether the data will be shared with any other organisations; • the fact that data subjects can withdraw their consent at any time; and • a recording of explicit consent (rather than implied), including the date when consent was given. 	Medium	30 June 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
13	<p>The Information Security Incident Reporting Policy will be reviewed and updated to cover:</p> <ul style="list-style-type: none"> • reference to General Data Protection Regulation (GDPR); • what constitutes a data breach; • how the severity of the data breach is to be assessed; • reporting and recording of near misses in addition to actual data breaches; • how to determine whether a data breach requires reporting to the ICO; • what information a data breach notification to the ICO should contain in line with ICO guidance; • how the data breach is to be notified to the ICO; • timescales for reporting a data breach to the ICO; • what to do if all information is not available to report to the ICO within 72 hours; • the requirement to notify individual affected by the breach under certain circumstances; • what information to provide to individuals when notifying them about a data breach in line with ICO guidance; and • consequences of failing to report a data breach. 	Medium	31 May 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)

14	<p>The Data Breach Log will be updated to cover:</p> <ul style="list-style-type: none"> • details of near misses in addition to breaches; • date the breach was reported internally (only the date that the breach occurred is currently recorded); • who reported the breach; • format of data lost/impacted; • source of data lost/impacted; • the categories of those affected by the breach (employees, service users etc.) and approximate number of individuals/records concerned for each category; • root cause of the breach; • whether the breach was notifiable to the ICO; • whether the breach was notified to the ICO within 72 hours (where relevant); • when the breach was notified to the individuals (where relevant); • when the breach was notified to the relevant management forum; • actions taken at the time of the breach/to respond to the breach; and • date remedial actions completed. 	Medium	31 May 2022	Alex Cowen - IT Business Development Manager (& Acting DPO)
15	<p>The Council will ensure that a register of third parties to whom 'in scope' (personal) data is transferred to is in place and records:</p> <ul style="list-style-type: none"> • name of the third party; • whether there will be sharing of personal data with the third party (if it is a general register for all third parties/contracts etc.); • whether a formal contract or other legal act is in place; • contract owner; • whether the contract contains the required contractual data confidentiality terms and conditions / clauses; • start and end dates of the contract; and • other contractual protections that have been put in place/assessed (especially where a contract is not in place), such as reviewing the third party's terms and conditions or privacy notices, or the use of a signed data/information sharing agreement. <p>In addition, the Council will ensure that any Terms and Conditions used within agreements are in line with ICO guidance, and that data sharing agreements cover:</p> <ul style="list-style-type: none"> • the purpose, or purposes, of the sharing, including aims and benefits; • the potential recipients or types of recipient of the data, the circumstances in which they will have access and their contact details; • procedures for including additional organisations in the data sharing arrangement and for dealing with cases where an organisation needs to be excluded from the sharing; 	Medium	31 March 2022	Clare Priest – Group Manager - Commercial



<ul style="list-style-type: none"> • the data to be shared, including permissions for certain data items (i.e. only to be accessed by trained staff); • basis for sharing (lawful basis); • data quality – accuracy, relevance, compatibility/usability etc.; • data security, including for the transmission of data; • retention of shared data, including procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules; • individuals’ rights – procedures for dealing with DPA or FOIA access requests (one staff member or organisation takes overall responsibility for ensuring that the individual can gain access to all the shared data easily), including a broad outline of the types of data normally released in response to either DPA or FOIA requests and the types of information in the FOIA publication scheme; • dealing with complaints or queries, from members of the public; • periodic review of effectiveness of the data sharing initiative and of the agreement that governs it; • procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally; • procedures for dealing with any breach of the agreement; and • sanctions for failure to comply with the agreement or breaches by individual staff. 			
--	--	--	--

<p>Creditors – 20.21/22</p>		<p>3 High 9 Medium 3 Low</p>
<p>AP Training</p> <p>All staff can access basic AP functions on Agresso, including raising requisitions and confirming the receipt of goods. However, there is currently no formal training for staff, instead there is a reliance on managers to provide informal training or for support to be requested via Freshdesk.</p> <p>Without formal training there is a risk AP functions are completed incorrectly, impacting the payment of invoices. This was evidenced by our testing, where we found issues with the retrospective raising of requisitions and delays in receipting goods.</p> <p>Where requisitions are raised after orders are placed, there is a risk that the Council is committed to expenditure that has not been suitably approved or where there is no budget available. Where there are delays in receipting goods, the Council is unable to make payments for invoices (until receipted) which may lead to reputational issues with suppliers and potential interest charges. (High)</p> <p>Purchase Requisitions</p> <p>Purchase requisitions are to be raised and approved prior to placing orders with suppliers. For a sample of 20 invoices paid since April 2021, we identified that requisitions were raised and approved after invoice dates in seven instances. Further investigation found one of these was acceptable</p>		

given that this was a utility bill, however requisitions should have been raised before ordering for the remaining six (totalling £916,235). Where requisitions are retrospectively raised, there is a risk that the Council is committed to unapproved expenditure and budget may not be available for this expenditure. In addition, there is a risk that payments may be delayed where requisitions are raised after invoices are received. **(High)**

New Supplier Set Up - Checks



When setting up new suppliers, checks to confirm there are no existing accounts (based on name, address and bank details) and to verify bank details should be completed as part of the workflow approval process within Agresso. For a sample of ten new suppliers set up since April 2021, we identified that there was no evidence of such checks being completed. We undertook our own checks, noting that two of the sample shared bank details with existing suppliers and a further one of the sample had the same address details. As such, duplicate supplier accounts had been set up.

Without completing verification checks for bank details, there is a risk of fraud where incorrect information is used to set up accounts. In addition, without searching against existing records, there is a risk duplicate supplier accounts are set up. Where there are duplicate accounts, duplicate payments may be made. **(High)**

Accounts Payable Handbook



At the time of our review the AP Handbook was only accessible in hard copy, having been removed from the intranet in 2020/21 to be updated. We have agreed management actions as part of the Creditors reviews in 2019/20 and 2020/21 to update the handbook content and ensure this is made accessible to staff.

Without the handbook, there is a risk staff have insufficient guidance on AP functions. This may result in processes being completed incorrectly, such as the retrospectively raising of requisitions and delays in confirming the receipt of goods identified by our audit testing. **(Medium)**

Agresso Guidance for Staff (Set up and Amendment of Suppliers)



Help cards and guidance materials can be found on the Freshdesk Knowledge Base section on the staff intranet. Through review of the available guidance in relation to supplier set up and amendments, we found that this included outdated references, did not clearly assign responsibilities for new supplier checks and did not define the process for amending supplier accounts. Without sufficient guidance for staff, there is a risk processes are delayed or completed incorrectly, as was evidenced by our testing of new and amended supplier accounts. **(Medium)**

AP Agresso Access



Access to specific Agresso functions (such as inputting invoices) is restricted to the P2P team. We were unable to confirm that access was suitably restricted given that a user access report was not provided over the course of our review. Where access is not appropriately restricted, there is a risk that inappropriate users have access to attempt unauthorised actions. **(Medium)**.

Goods Receipt and Invoice Payment



Invoices are paid following the completion of a three-way match to confirm purchase order numbers (generated once requisitions are approved), receipt of goods and invoices received. We identified that seven of our sample of 20 invoices paid since April 2021 had not been paid in a timely manner, in line with stated payment terms. Although explanations were noted for five, the remaining two payments were delayed due to the untimely receipt of goods. There is a risk that invoices not paid in line with supplier payment terms incur additional charges for the Council. **(Medium)**

Supplier Account Amendments



Supporting evidence of checks to confirm requests for supplier amendments are uploaded onto Agresso and reviewed prior to these being approved by the P2P team. For a sample of 10 supplier accounts updated since April 2021, we were unable to confirm the nature of amendments made in two instances (given the limited supporting evidence and lack of a log). We noted there was no amendment log maintained and supporting evidence was insufficient (one instance) or not uploaded (one instance). Where amendments made to accounts cannot be confirmed, there is a risk inappropriate changes are made as a result of the limited audit trail. This could result in fraudulent payments being made. **(Medium)**

Expenditure Level Approvers



The Agresso system is designed to restrict approval access permissions for expenditure based on cost centre and value (levels range from one to four). We obtained a report detailing current level one, two, three and four approvers. We identified five from a sample of ten level one, two and three approvers were former staff members, whilst one of the two level four approvers had also left the Council. The requisition approval process follows an escalation system, with approval requests escalated to the next approver after eight days. Where approvers are former staff members, there is a risk of delays in approving requisitions, which may delay placing orders or result in staff placing these without approval.

In addition, where former staff remain approvers and retain access to logon, there is a risk unauthorised access to the system and expenditure is approved. **(Medium)**

Reconciliations



Transaction reports extracted from the accounts payable ledger were previously reconciled against the general ledger to identify discrepancies, such as inaccurate remaining supplier balances. Following the restructure and turnover of finance staff, these reconciliations have not been completed since May 2021. Where AP reconciliations are not completed, there is a risk that variances are not identified and investigated in a timely manner. **(Medium)**

Duplicate Supplier Accounts



As part of the Creditors reviews in 2019/20 and 2020/21, we agreed management actions with regards to reviewing potential duplicate supplier accounts identified by data analytics testing. We were informed by the Interim Head of Transactional Finance this had not yet been done. We completed data analytics using the supplier Masterfile, identifying 528 accounts with shared names, 713 with similar names and 966 with shared bank details. Without ensuring duplicate supplier accounts are identified and removed as appropriate, there is a risk that duplicate payments may be made (as was identified by our Supplier Duplicate Payments 2021/22 review). **(Medium)**

Shared Bank Details – Supplier and Payroll Records



We completed data analytics testing to identify whether there were any supplier accounts that had the same bank details with Council staff (as per payroll records). We noted there were 27 supplier accounts set up with bank details also used to pay Council staff in 2021/22. Through review of a report of invoices paid since February 2016, we identified that payments had been made to 19 of these supplier accounts (150 payments totalling £378,687). We were unable to confirm why these accounts had been set up at the time of our audit testing. This was in part as our requests were not responded to as well as the requirement to issue this report in a timely manner due to the significant issues identified.

Where there are supplier accounts inappropriately set up with bank details shared with staff, there is a risk that fraudulent payments may be made. **(Medium)**

1	The Interim Head of Transactional Finance will agree a timeframe for updating the AP Handbook. Once updated, the handbook will be uploaded onto the intranet and staff will be informed of its location.	Medium	31 December 2022	Jasvinder Dalvair
2	The guidance available to staff relating to new suppliers will be reviewed and updated to reflect current responsibilities and expectations. Guidance will also be prepared to outline the process for making amendments to supplier accounts, including adding backing documentation, completing verification checks and approvals.	Medium	31 December 2022	Jasvinder Dalvair
3	The Council will review all users with Agresso AP access to confirm: <ul style="list-style-type: none"> • Users are current staff members; and • Access is appropriate based on job roles. Access will be removed or amended if any anomalies are identified.	Medium	31 December 2022	Jasvinder Dalvair
4	Accounts payable functions on Agresso will be included in the finance training programme to be implemented for staff. Training will be a requirement before system access is granted.	High	30 September 2022	Jasvinder Dalvair
5	The Council will prepare an exceptions list detailing those instances where it is acceptable for requisitions to be raised after invoices are received. Consideration will be made for how the timely raising of requisitions can be monitored (monthly reporting or system solution).	High	30 September 2022	Jasvinder Dalvair
6	Registered invoice lists, detailing all invoices that have been received but not yet paid owing to delays in requisitions / receipting goods, will be prepared on a periodic basis by the Interim Head of Financial Transactions. Reports will be reviewed by the P2P team and direct contact made with relevant staff to ensure required actions are completed (to allow payment).	Medium	30 September 2022	Jasvinder Dalvair
7	The Council will implement a process to ensure the following checks are completed when setting up new supplier accounts: <ul style="list-style-type: none"> • Checks for supplier names against existing supplier accounts; • Checks for supplier addresses against existing supplier accounts; • Checks for bank details against existing supplier accounts; and • Checks to verify the bank details being input for new supplier accounts. 	High	30 September 2022	Jasvinder Dalvair

	Accounts will not be set up until all checks are fully completed and a record of these checks will be retained.			
8	P2P team members will be informed that supporting documentation must be added where amendments are made to supplier accounts. Where supporting documentation does not clearly indicate the type of change, a note will be added to explain this. As part of this, P2P team members responsible for reviewing and approving amendments via the workflow will confirm sufficient supporting documentation (and notes) have been added to fully explain the nature of the change.	Medium	30 September 2022	Jasvinder Dalvair
9	The Council will implement a process to detect 'level approval rights' for departing staff members and reassign these appropriately (either to replacements or another suitable staff member). This will include removing current level approval permissions from former employees.	Medium	31 December 2022	Ade Adewumi
10	An appropriate member of the Finance Team will be assigned to complete monthly accounts payable reconciliations, as well as a second staff member to check and sign these off. The preparation of the accounts receivable reconciliations will resume, including retrospectively completing all for 2021/22.	Medium	30 November 2022	Jasvinder Dalvair
11	The Interim Head of Transactional Finance will complete a periodic exercise to review potential duplicate supplier accounts (based on names and bank details) and remove those identified as duplicates. This will include in the first instance reviewing those duplicates identified by our findings above.	Medium	30 September 2022	Jasvinder Dalvair
12	The Council will review those 27 supplier accounts which share bank details with Council staff. Appropriate action will be taken if issues are identified. Accounts will be removed as appropriate based on this review.	Medium	30 September 2022	Ade Adewumi

Cyber Essentials – 29.21/22	Advisory (significant weaknesses)	4 High 15 Medium 1 Low
Slough Borough Council completed a self-assessment questionnaire on 2 February 2022. Based upon the evidence available at the time of our fieldwork, we found that ten of the 50 requirements from the five Cyber Essentials control themes had evidence to support the self-assessment that controls are established.		



Of the remaining 40 requirements, four were self-assessed as implemented but not tested, seven were not applicable; and issues were identified in the remaining 29. For 19 of the remaining 29 cases, we agreed with the organisation's assessment that these areas had not been implemented, as noted in Appendix B of the report. For 10 of the 29 cases, we determined that the evidence provided did not fully support the self-assessment by the Council.

These issues were identified across the Office Firewalls and Internet Gateways, Secure Configuration, Security Update Management, Malware Protection and User Accounts and Administrative Accounts control themes.

We have not included the detail of the weaknesses due to the sensitive nature of this work, but this has been shared internally with relevant Council staff.

APPENDIX B - SUMMARY OF PROGRESS TO DATE

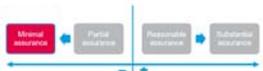
The table below provides a status update on the summary of progress with the 2021/22 internal audit plan to date.

2021/22 Internal Audit Plan

Assignment area	Fieldwork date/status	Draft report	Final report	Opinion	Actions		
					L	M	H
IT Business Continuity	Final Report	15 July 2021	17 September 2021	Advisory (significant weaknesses)	2	6	1
General Ledger	Final Report	23 November 2021	5 January 2022		1	4	6
Business Continuity and Disaster Recovery	Final Report	8 September 2021	22 October 2021		3	7	1
Children Missing Education (CME)	Final Report	1 July 2021	25 August 2021		3	5	3
Debtors Management	Final Report	11 January 2022	1 February 2022		3	5	4
Follow Up Q1	Final Report	8 September 2021	20 th January 2022	Little Progress	7	2	0



Council Tax	Final Report	10 November 2021	16 December 2021		4	1	3
Rent Arrears Recovery	Final Report	14 July 2021	10 August 2021		5	3	0
School Reviews - Pippins	Final Report	23 July 2021	8 October 2021		8	6	0
Rent Accounts	Final Report	8 December 2021	21 December 2021		6	2	2
Whistleblowing	Final Report	16 November 2021	10 December 2021		2	3	1
School Reviews - Cippenham	Final Report	5 July 2021	20 August 2021		3	1	0
Schools Review – Claycots School	Final Report	29 September 2021	20 October 2021		3	3	0
Housing Benefit	Final Report	19 November 2021	16 December 2021		3	2	0

Travel Demand Management Grant	Final Report	14 May 2021	14 May 2021	Advisory	0	0	0
Follow Up Q2	Draft Report	24 September 2021					
Supplier Duplicate Payments - (Part 1)	Final Report	9 November 2021	5 April 2022	Advisory (Significant Weaknesses)	0	0	2
Payroll	Draft Report	10 November 2021					
Risk Management	Final Report	11 January 2022	5 July 2022		3	6	2
Temporary Accommodation Strategy	Final Report	18 January 2022	16 March 2022		3	7	7
Creditors	Final Report	18 January 2022	18 July 2022		3	9	3
Assets	Draft Report	31 January 2022					
Capital Expenditure	Final Report	15 February 2022	17 May 2022		3	7	2
GDPR	Final Report	15 February 2022	25 April 2022	Advisory (significant weaknesses)	1	12	3
Business Rates	Draft Report	21 February 2022					



Follow Up Q3	Draft Report	7 March 2022					
Supplier Duplicate Payments - (Part 2)	Draft Report	3 May 2022					
Cyber Essentials	Final Report	12 April 2022	18 July 2022	Advisory (significant weaknesses)	1	15	4
Schools Audit – Priory	Draft Report	24 March 2022					
Matrix	Draft Report	28 April 2022					
RMI Contract Management	Draft Report	11 April 2022					
Leasehold Service Charges	Draft Report	18 May 2022					
Slough Children First – Governance	Draft Report	16 May 2022					
Corporate Health and Safety	Draft Report	28 April 2022					
Follow Up Q4	Draft Report	12 May 2022					
Capital Projects – Britwell GP Hub	Draft Report	13 May 2022					
Treasury Management*	Defer to 22/23						
Slough Children First – VFM	Draft Report	14 June 2022					
Subsidiary Company Governance*	Defer to 22/23						
Medium Term Financial Planning	Defer to 22/23						

Budget Setting and Control

Defer to 22/23

Our Futures

Replaced with Supplier
duplicate payments pt 2

* Please refer to section 3.3 above for details on these reviews

The table below provides a status update on the summary of progress with the 2022/23 internal audit plan to date.

2022/23 Internal Audit Plan

Assignment area	Fieldwork date/status	Draft report	Final report	Opinion	Actions		
					L	M	H
Treasury Management	In progress						
Subsidiary Company Governance	Draft	14/7/22					
Medium Term Financial Strategy	In QA						
Budget Setting and Control	In QA						
Workforce - Recruitment and Retention	In progress						
Children Missing Education	27 July 2022						
Adult Social Care Transformation	16 August 2022						
Follow up Q2	30 August 2022						



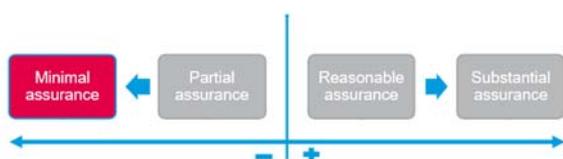
IT Business Continuity	September 2022
Risk Management	5 September 2022
Payroll (inc Data Analytics)	7 September 2022
Rent Accounts	21 September 2022
Council Tax	26 September 2022
General Ledger	4 October 2022
Creditors	14 October 2022
Temporary Accommodation	25 October 2022
Housing Benefits	1 November 2022
Payroll and HR Interface	21 November 2022
Whistleblowing	5 December 2022
Rent Accounts Recovery	12 December 2022
Corporate Health and Safety	3 January 2023
Business Rates	16 January 2023
Debtors	19 January 2023



Capital Expenditure	30 January 2023
Cyber Essentials	1 February 2023
Assets	2 February 2023
Treasury Management	27 February 2023
Follow up Q4	13 March 2023
Strategic Housing Management	16 March 2023

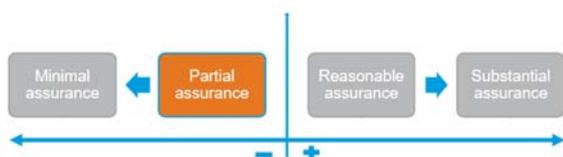
APPENDIX C: 2021/22 ASSURANCE OPINIONS

We are constantly developing and evolving the methods used to provide assurance to our clients. As part of this, we have refreshed our opinion levels in line with the graphics below. We use the following levels of opinion classification within our internal audit reports, reflecting the level of assurance the Council can take:



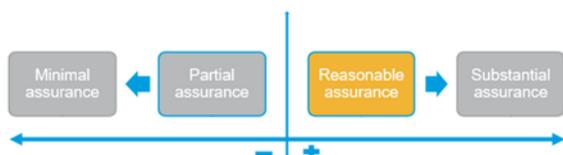
Taking account of the issues identified, the Council can take minimal assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

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



Taking account of the issues identified, the Council 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).



Taking account of the issues identified, the Council 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).



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

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Daniel.Harris@rsmuk.com

Anna O’Keeffe, Senior Manager

Anna.Okeeffe@rsmuk.com

Fiona Ho, Manager

Fiona.Ho@rsmuk.com

THE POWER OF BEING UNDERSTOOD AUDIT | TAX | CONSULTING

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, and RSM UK Consulting LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.

RSM UK Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317.