



WEST LINDSEY DISTRICT COUNCIL

IT Operations

Final Internal Audit Report: 1.24/25

5 September 2024

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.

CONTENTS

Audit outcome overview	3
Summary of management actions	5

Appendices

Detailed findings and actions	7
Appendix A: Categorisation of findings	13
Appendix B: Scope	14





AUDIT OUTCOME OVERVIEW

In line with our scope, included at Appendix B, the overview of our findings is detailed below.

Conclusion: Our audit has found that, overall, the Council has adequate controls in place with regards to the infrastructure estate that is spread across two data centres in Gainsborough and Sleaford. The Council utilises a variety of different monitoring tools across the server estate and employ a high availability connection between servers of the two data centres such that servers in one data centre could failover to the other.

However, whilst it was noted that Business Impact Assessments (BIA) are presently being undertaken throughout the Council, we noted that the present Business Continuity Plan was out of date and not originally designed with the necessary Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). In addition, scheduled backup restore testing, is not undertaken.

Internal audit opinion:

 Minimal Assurance	 Partial Assurance	 Reasonable Assurance	 Substantial Assurance	<p>Taking account of the issues identified, the board can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.</p> <p>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).</p>
--	--	---	--	--

Audit themes: Policies and / or procedures

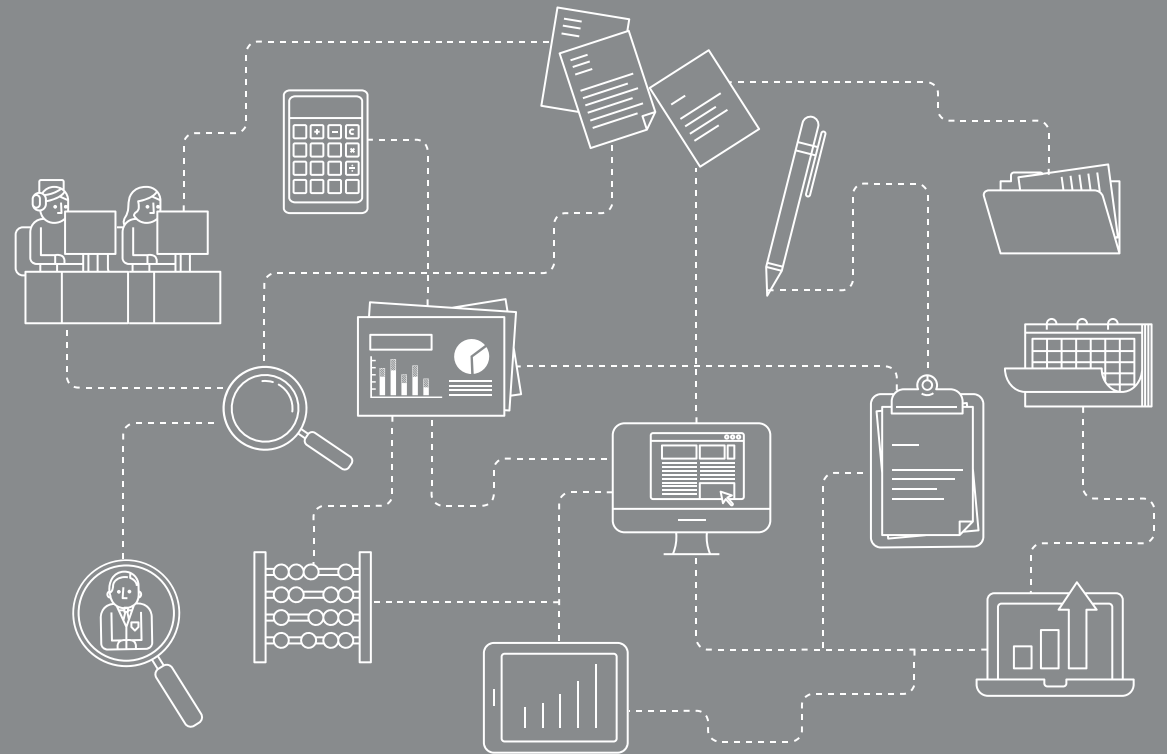
- The Business Continuity Plan (BCP) was last reviewed in 2022 and therefore the review of this document was overdue. We also noted that the BCP did not include recovery point objectives (RPO) or recovery time objectives (RTO). **(Medium)**
- Through review of the Backup Management section of the ICT Disaster Recovery Policy, we identified areas for improvement to enhance the detail and quality of the policy, including provisions for encrypting all backups to ensure data security and conducting periodic backup data restore testing. **(Medium)**

Planning

- At the time of the audit, Council departments were still in the process of completing their Business Impact Analysis (BIA) and therefore at present these have not informed the Business Continuity Plan. **(Medium)**

Summary of Actions for Management

01



SUMMARY OF MANAGEMENT ACTIONS

The action priorities are defined as*:

High

Immediate management attention is necessary.

Medium

Timely management attention is necessary.

Low

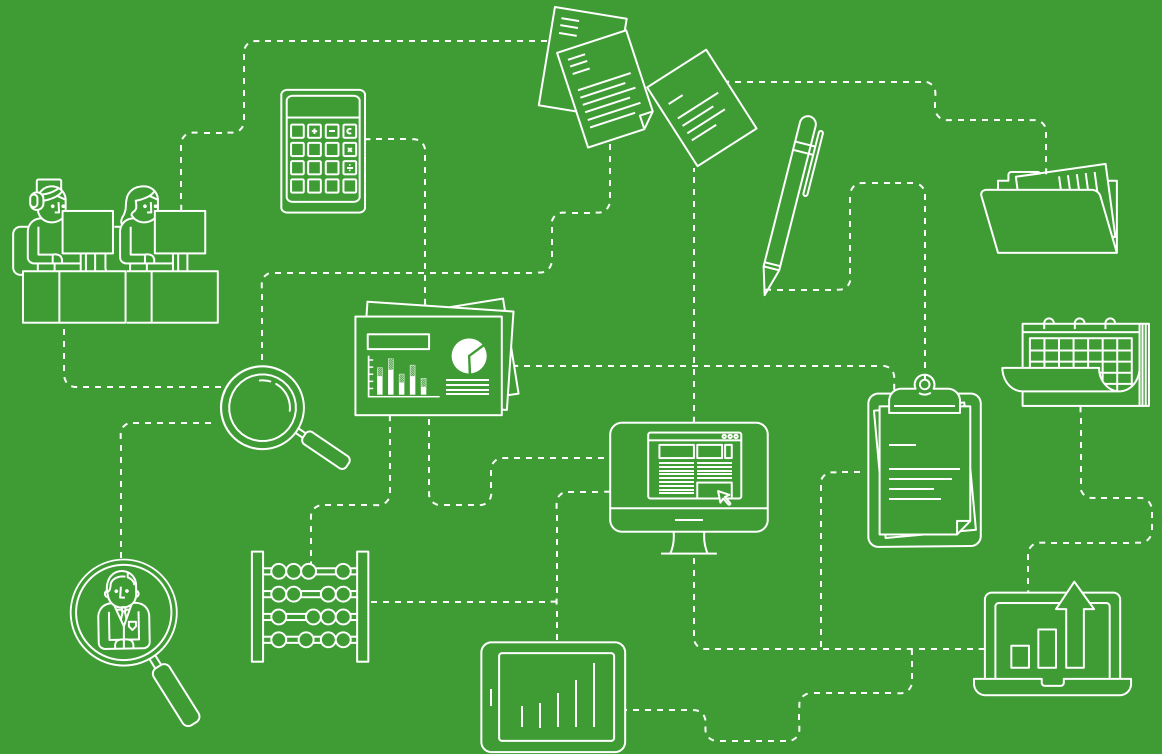
There is scope for enhancing control or improving efficiency.

Ref	Action	Priority	Responsible Owner	Date
1	The hardened standard baseline build for servers will be formally documented and approved.	Low	ICT Manager	31 October 2025
2	The West Lindsey/North Kesteven Network Topology Diagram will be updated to accurately reflect the high availability pair firewalls and all current network configurations	Low	ICT Manager	31 October 2025
3	<p>The Backup Management section of the ICT Disaster Recovery Policy will be updated to include provisions for:</p> <ul style="list-style-type: none"> • Encrypting all backups to ensure data security; • Implementing periodic testing of backups to verify data integrity and functionality; and • Establishing a process for regular review of backup logs with documented evidence of these reviews. <p>Moreover, backup data restore testing will be conducted on a scheduled and/or rotational basis to validate that data will be recoverable in the case of a disaster.</p>	Medium	ICT Manager	31 October 2025
4	Business Impact Assessment (BIA) templates will be completed by each department by the end of August 2024 in line with management expectation. Key department stakeholders will be involved and consulted during this process to identify key business processes, systems and operational dependencies will be identified. Moreover, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) will be defined for each key system.	Medium	Emergency Planning & Business Continuity Officer	Completed
5	The Business Continuity Plan (BCP) will be reviewed and approved in line with the review period. Furthermore, once the BIA's have been completed, the BCP will be updated to include the RPO's and RTO's for each key process and system including operational dependencies. The plan will be tested annually to ensure that all key stakeholders know their role and responsibility in the business continuity process. Where applicable, the BCP will be updated to reflect results of the test.	Medium	Emergency Planning & Business Continuity Officer	31 March 2025

* Refer to Appendix B for more detail

Detailed Findings and Actions

02



DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all audit testing undertaken.

Background / Why we did the audit

A recent survey by the Local Government Association revealed that councils face an average of 800 cyber-attacks per hour, underscoring the urgent need for robust cybersecurity measures. Over the past two years, the Council has conducted several ICT audits covering Disaster Recovery, Cyber Security, Patching, and Incident Management. To minimise duplication, this audit specifically targeted the datacentre and server estate.

The Council commissioned this audit to ensure its ICT infrastructure is secure, resilient, and capable of supporting critical operations. This review focused on resilience, operating systems and firmware management, security standards, network segregation, backup and recovery processes, monitoring tools, and privileged access control. Regular updates and secure configurations protect against vulnerabilities, while effective network segregation and isolation of outdated systems enhance security. Reliable backups and regular testing are crucial for data recovery. Continuous monitoring aids in early threat detection, and strict access controls prevent unauthorised access. Failure to address these areas could lead to unauthorised access, data breaches, and operational disruptions, posing significant risks to the council's operations and reputation.

Area: Hardened Standard Build

Control	The server standard build template is configured in the server management software to deploy to servers, however, the standard build has not been documented.	Assessment: Design × Compliance -			
Findings / Implications	Management demonstrated in a walkthrough that four template options for server endpoint builds are stored in the deployment programme in the server management software, vCenter (VMware VSphere). However, whilst configuration templates for the hardened standard builds of servers have been established, these have not been formally documented and approved. This increases the risk of an inconsistent approach to application of the standard build which could lead in configuration errors, applications failures and security vulnerabilities.				
Management Action 1	The hardened standard baseline build for servers will be formally, documented and approved.	<table border="0"> <tr> <td data-bbox="1388 1308 1635 1428">Responsible Owner: ICT Manager</td> <td data-bbox="1635 1308 1926 1428">Date: 31 October 2025</td> <td data-bbox="1926 1308 2119 1428">Priority: Low</td> </tr> </table>	Responsible Owner: ICT Manager	Date: 31 October 2025	Priority: Low
Responsible Owner: ICT Manager	Date: 31 October 2025	Priority: Low			

Area: Network Segregation

Control	A Network Topology Diagram of the technology environment has been documented.	Assessment:	
		Design	✓
		Compliance	×

Findings / Implications We reviewed the West Lindsey/North Kesteven Network Topology Diagram and noted that, although it was last reviewed in April 2024, it did not depict the HA firewall pair present within the network, and we were advised that the diagram was not a fully accurate representation as a result of the missing firewalls. This increases the risk of misconfiguration during network changes or troubleshooting which could lead to extended network downtime. In mitigation, we noted that a full view of the current network set-up was available through the system management software in use.

Management Action 2	The West Lindsey/North Kesteven Network Topology Diagram will be updated to accurately reflect the high availability pair firewalls and all current network configurations.	Responsible Owner: ICT Manager	Date: 31 October 2025	Priority: Low
----------------------------	---	--	---------------------------------	--------------------------------

Area: Server Estate Backups and Testing

Control	An approach to backup management is documented within the ICT Disaster Recovery Policy, however the policy is not comprehensive.	Assessment:	
		Design	×
		Compliance	-

Findings / Implications Through inspection of the backup management section within the ICT Disaster Recovery policy we noted that it describes the daily VEEAM backup process, and backup retention arrangements. However, the policy does not include guidance around the encryption of backups, periodic testing of backups, and the review of backup logs. This omission could lead to potential unauthorised access to backup data, undetected issues with backup integrity, and the inability to recover data in the event of an incident. Additionally, we were unable to ascertain whether data backup restores are conducted.

There is a risk that the Council may not be able restore data in time following a disaster which could result in prolonged downtime, data loss, financial losses, and reputational damage

Management Action 3	<p>The backup management section of the ICT Disaster Recovery Policy will be updated to include provisions for:</p> <ul style="list-style-type: none"> • Encrypting all backups to ensure data security; • Implementing periodic testing of backups to verify data integrity and functionality; and • Establishing a process for regular review of backup logs with documented evidence of these reviews. <p>Moreover, backup data restore testing will be conducted on a scheduled and/or rotational basis to validate that data will be recoverable in the case of a disaster.</p>	Responsible Owner:	Date:	Priority:
		ICT Manager	31 October 2025	Medium

Area: Business Continuity Planning

Control	Council-wide business impact assessments have not been conducted.	Assessment:		
		Design		×
		Compliance		-
Findings / Implications	<p>Management informed us that the Council, at the time of the audit, was in the process of conducting Business Impact Analysis (BIA) to gauge maximum tolerable downtimes, key business processes, key business systems, and Recovery Point Objectives (RPOs). We were informed that that all departments within the Council are in the process of completing business impact assessment templates by the end of August 2024.</p> <p>If RPOs and Recovery Time Objectives (RTOs) for critical business systems, processes and operational dependencies are not defined and used to determine the prioritisation for the recovery of systems in the event of an incident, there is a risk of inadequate preparedness and response during disruptions, potentially leading to prolonged downtime and data loss.</p>			
Management Action 4	Business Impact Assessment (BIA) templates will be completed by each department by the end of August 2024 in line with management expectation. Key department stakeholders will be involved and consulted during this process to identify key business processes, systems and operational dependencies will be identified. Moreover, Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) will be defined for each key system.	Responsible Owner: Emergency Planning & Business Continuity Officer	Date: Completed	Priority: Medium

Area: Business Continuity Planning

Control	A Business Continuity Plan has been established; however, it has not been recently reviewed.	Assessment:		
		Design		✓
		Compliance		×
Findings / Implications	<p>We inspected the Business Continuity Plan (BCP) and noted that the document is overdue for review having last been reviewed in January 2022. We noted that that the plan was due to have been reviewed in June 2023 and there is no evidence to indicate that it has been reviewed in the last 12 months. Additionally, details around roles and responsibilities and testing of the plan are not included in the document. Through our review, we further noted that the BCP did not include RPOs or RTOs. The lack of appropriate guidance could lead to confusion and inefficiency in resolving an incident, potentially resulting in prolonged downtime, financial loss, and reputational damage.</p>			
Management Action 5	The BCP will be reviewed and approved in line with the review period. Furthermore, once the BIA's have been completed, the BCP will be updated to include the RPO's and RTO's for each key process and system including operational dependencies.	Responsible Owner: Emergency	Date: 31 March 2025	Priority: Medium

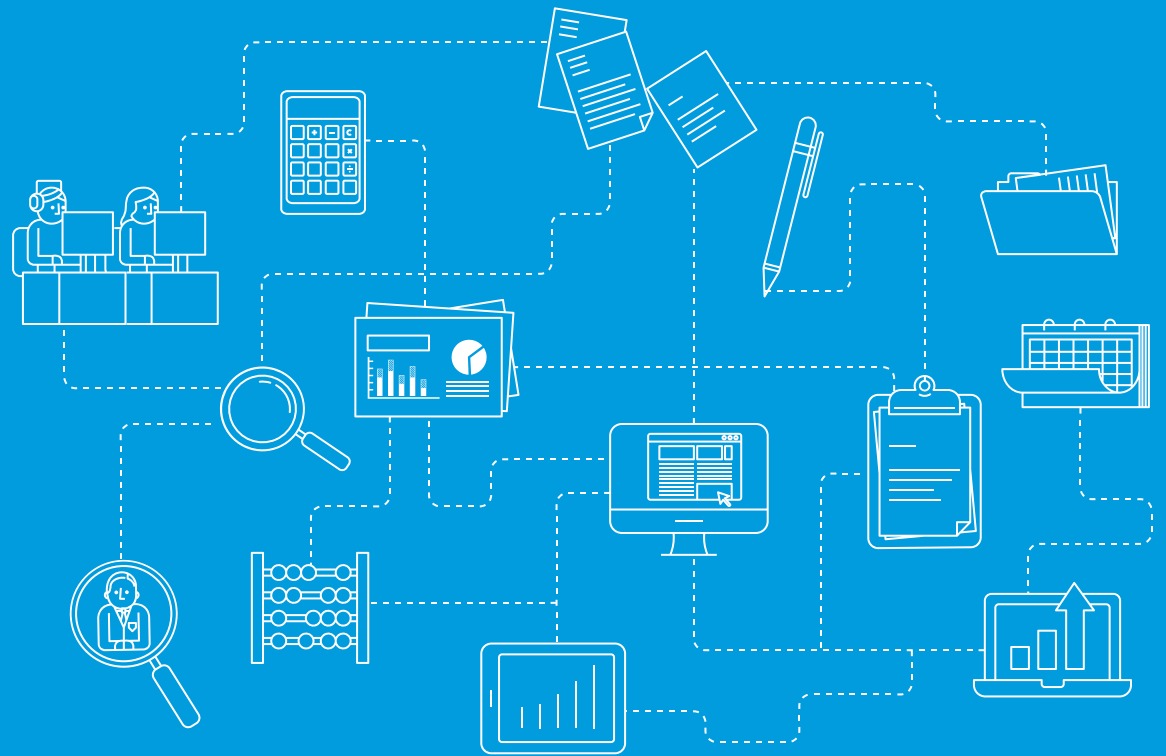
Area: Business Continuity Planning

The plan will be tested annually to ensure that all key stakeholders know their role and responsibility in the business continuity process. Where applicable, the BCP will be updated to reflect results of the test.

Planning &
Business
Continuity Officer

Appendices

03



APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings

Low

There is scope for enhancing control or improving efficiency.

Medium

Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.

High

Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

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

Area	Control design not effective*	Non-compliance with controls*	Agreed actions		
			Low	Medium	High
Hardened Standard Build	1	0	1	0	0
Network Segregation	0	1	1	0	0
Server Estate Backups and Testing	1	0	0	1	0
Business Continuity Planning	1	1	0	2	0
Total			2	3	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the objective

Objective of the review	Risks relevant to the scope of the review	Risk source
The objective of the review is to consider the extent to which management have plans in place to ensure that the infrastructure is robust and fit for purpose and operates in a secure environment to identify areas which may require further management attention or investment.	ICT Security and Information Governance arrangements are ineffective	Strategic risk register

When planning the audit, the following were agreed:

- Resilience has been built into the datacentre to provide power and an internet connection should the primary source be lost, this includes the use of an Uninterruptible Power Source (UPS) and environmental controls.
- Management have visibility of the Operating Systems (OS) and firmware of the server estate to confirm that it is up to date and within support.
- A hardened standard build has been documented and used across the server estate, considering security control frameworks and benchmarks (such as CIS (Centre for Internet Security)).
- The ICT network has been segregated to provide strength in depth and to segregate any End of Life (EoL) servers, databases or applications. This may include the use of a DMZ (Demilitarised Zone).
- Backups of the server estate are run and restore testing is conducted against established BCP plans providing ICT with an agreed list of Council systems to be recovered together with their priority and expected timescales for system restore.
- Monitoring and alerting tools are established across the server estate, such as anti-virus, Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tools.
- Privileged access to the datacentre and servers is controlled and based on the principle of least privilege.

Limitations to the scope of the audit assignment:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of ICT infrastructure, ICT controls or ICT security.
- This audit will look at how the server estate and datacentre is managed in respect to West Lindsey District Council and we will not review how controls apply to North Kesteven District Council.

- The approach taken for this review will be to validate the design of key controls and will not include all monitoring controls.
- We will be testing only selected key controls on a walkthrough-basis only.
- We will not perform penetration tests and vulnerability assessments.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the ICT environment, and it will be necessary for management to consider the results and make their own judgement on the risks and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- Our work will not provide an absolute assurance that material errors, loss or fraud do not exist.

Debrief held 23 July 2024
Last evidence received 25 July 2024
Draft report issued 8 August 2024
Responses received 5 September 2024

Final report issued 5 September 2024

Internal audit Contacts Rob Barnett, Head of Internal Audit
 Aaron Macdonald, Internal Audit Manager
 Anna O’Keeffe, National IT Audit Director
 Kolisa Benelwa, Manager, Technology Risk Assurance (TRA)
 Graeme Clarke, Senior Consultant (TRA)
 Abdu-Allah Awad, Consultant (TRA)

Client sponsor Nova Roberts, Director, Change Management, ICT and Regulatory Services

Distribution Nova Roberts, Director, Change Management, ICT and Regulatory Services
 Cliff Dean, ICT Shared Services Manager

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

FOR FURTHER INFORMATION CONTACT

Rob Barnett, Head of Internal Audit

Email: Robert.Barnett@rsmuk.com

Telephone: +44 115 964 4520

Aaron Macdonald, Manager

Email: Aaron.Macdonad@rsmuk.com

Telephone: +44 115 964 4517

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of West Lindsey District Council, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. 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 and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.