

Final Internal Audit Cyber Report

ISO 27001 Annex A Gap Analysis

October 2024

Distribution:

- Chief Digital Officer
- Interim Assistant Chief Executive
- Head of Specialist Systems
- Head of Digital Operations
- Cyber Security Manager
- Director of Finance & Deputy S151 (Final report only)
- Corporate Director Resources and S151 (Final report only)

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

Confidentiality and Disclosure Clause

This report ("Report") was prepared by Forvis Mazars LLP at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Forvis Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations, and confidentiality.

Executive Summary

1. Introduction	3
2. Key Issues	4

Detailed Report

3. Actions and Key Findings/Rationale	5
---------------------------------------	---

Appendices

1. Terms of Reference
2. Definitions for Audit Opinions and Identified Issues
3. Statement of Responsibility

1. Introduction

- 1.1. London Borough of Croydon (the Council) is undergoing a period of change from both an organisational and cyber security perspective. Its current Information Security Policy framework has been developed towards the Council's implementation and maintenance of an Information Security Management System (ISMS).
- 1.2. The Council's ISMS is currently based on alignment with the security control baselines set out in Annex A of the ISO/IEC 27001.
- 1.3. ISO/IEC 27001 is an internationally recognised standard which defines the baselines to manage information security risks. The standard was updated in 2022 (ISO/IEC 27001:2022) from the previous 2013 version to help ensure that prescribed security controls remained relevant and robust in managing security risks in a changing cyber security landscape.
- 1.4. This internal audit focussed on reviewing the Annex A of ISO/IEC 27001:2022 (ISO 27001) against the controls in the Council's security policy framework to establish whether there was appropriate alignment.
- 1.5. While the review was performed remotely, all relevant documents required to complete the review were obtained.
- 1.6. Adequate and effective compliance with ISO 27001 could not be demonstrated following review of documentation provided and stakeholder discussion during the internal audit.
- 1.7. Governance of the Council's ISMS (to safeguard assets, including people, information, and infrastructure) and demonstration of top management commitment to Information Security required some improvement.
- 1.8. While not all the controls set out in Annex A may require an equal level of definition and documentation, an in-depth review of the Council's current arrangements against the Annex A of ISO 27001 is necessary to identify and implement the controls which are suitable to enhance the Council's security posture. Discussion noted that plans by the Information Security Manager and Data Protection Officer (DPO) were in progress to review the current security arrangements and implement suitable alignment with ISO 27001. It is considered that for adequate and effective Information security to be achieved within the Council, there should be ongoing collaboration between the Information Security Manager and stakeholders across the organisation.
- 1.9. The audit was undertaken as part of the agreed Internal Audit Plan for 2023/24. The objectives, approach and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 1 Issues

Planned reviews were not provided for in the policy and there was no evidence of reviews being undertaken previously to help ensure the Council's specific ISMS remained relevant and effective. **(Issue 1)**

There were no defined and documented incident response and recovery processes and procedures dedicated towards requirements for information security in line with ISO 27001. **(Issue 2)**

There were no identifiable processes in place to help ensure that Information Security policies were read and understood by relevant personnel as well as being easy to access. Regular and appropriate training on information security was not effectively implemented. **(Issue 3)**

Technological controls were not defined, documented, and uniformly implemented in line with ISO 27001. These included gaps relating to anti-malware deployment and vulnerability management **(Issue 4)**

Priority 2 Issues

There were no comprehensively defined and documented identity and access management (in terms of access to the Council's logical and physical assets) processes and procedures in line with ISO 27001. **(Issue 5)**

Comprehensively defined and documented processes and procedures to manage information security requirements and mitigate any risks associated with suppliers' access to assets across the Council were not in place. **(Issue 6)**

Procedures for operational activities related to information security which may need to be documented and enforced had not been identified and implemented in line with ISO 27001. **(Issue 7)**

Defined and documented processes and procedures related to physical access, environmental protection of information and secure facilities needed to be reviewed, appropriately developed, and enforced in line with ISO 27001. **(Issue 8)**

There were no priority 3 issues identified.

3. Actions and Key Findings/Rationale

Control Area 1: Review of Information Security Policy and Procedures

Priority	Action by Management	Detailed Finding/Rationale - Issue 1
1	<p>Majority of policies are now reviewed by the Information Security Manager, with input from technical resource and senior management where needed. Broken links have been checked/amended and they have been checked for their alignment to the ISO27001 2022 standards. Review dates and ownership have been updated in the policy management platform. All policies referenced are available in the platform. The policy management platform also includes functionality to ensure policies remain in an annual cycle for review. Remaining policies to be reviewed in September - expected completion by end of</p>	<p>Expected Control</p> <p>Policies are aligned with the Annex A of ISO 27001 controls and be reviewed periodically to help ensure the Council’s specific ISMS is relevant, appropriately defined, documented, and uniformly implemented across the Council to achieve tailored information security and effective risk management.</p> <p>Finding/Issue</p> <p>There was absence of a complete, defined and up to date security policy, which had been periodically reviewed to align with relevant aspects of the following four control groups of ISO 27001:</p> <ol style="list-style-type: none"> 1. Organisational controls: 37 controls pertaining to organisational policies, procedures, and processes to achieve effective information security. 2. People controls: 8 controls pertaining to the personnel related aspects of information security. 3. Physical controls: 14 controls related to physical access, environmental protection of information and secure facilities. 4. Technological controls: 34 controls to achieve a secure IT infrastructure.

	<p>October 2024. Further to this – a full process of communication to the relevant personnel is planned, to ensure that adherence to policies which affect various roles is in place. This should also be manageable through the policy platform, although other methods (email communication and viva engage messages) will also be considered.</p>	<p>There were five policies provided for the review (Information Security and Information Management Policy, Acceptable Use Policy (AUP), Workforce Data Protection Policy, Data Protection Policy, and a Detailed Information Security Standard (in draft).</p> <p>However, there was no evidence that reviews of the existing policies had been previously planned or performed. In addition, from review of the policies, all the links provided were broken links and none of the additional policies cited within these were available. There was also no evidence from review of the Workforce Data Protection Policy that it had been formally approved by management.</p> <p>Furthermore, it was identified that, although the policies (including the draft Detailed Information Security Standard) were undergoing review and revision, the ongoing review was based on alignment to the ISO/IEC 27001 issued in 2013 and not the latest version updated in 2022. Arrangements to update relevant policies to the 2022 version of ISO27001 had not yet commenced as approval to purchase the Standard had not been settled.</p>
Responsible Officer	Deadline	Risk
David Wood	31/10/2024	<p>Without regular/planned policy reviews, and revision where appropriate, the organisation may fail to effectively and adequately adapt safeguards to protect the organisation against the evolving cybersecurity threat landscape, thereby increasing risk exposure.</p>

Control Area 1: Information Security Event Management

Priority	Action by Management	Detailed Finding/Rationale - Issue 2				
1	<p>Incident management is currently only done on a small scale at the IT Helpdesk level. A full incident management plan/procedure is in progress of development to guide the organisation through incident readiness, and this will be tested when appropriate. This is also being matched with a review of the ITDR capabilities, to ensure it meets the organisation's wider expectations, and is in line with the BIAs for the business areas, and for CDS themselves.</p>	<p>Expected Control</p> <p>Information Security incidents are managed by defining, establishing, documenting, and communicating information security incident management processes, procedures and roles and responsibilities to ensure quick, effective, consistent, and orderly response to information security incidents, including communication on information security events.</p> <p>Finding/Issue</p> <p>Security incidents were to be reported to the IT Helpdesk (Littlefish) who had their defined response process in place for reported incidents.</p> <p>However, although Littlefish may need to escalate some security incidents to the information security function of the Council, the Council lacked defined and documented incident response processes and procedures dedicated towards requirements for information security. In addition, the procedure required for the Council's personnel to report incidents were not clear and well documented.</p> <p>Similarly, there were no dedicated information security processes and procedures documented for business continuity and disaster recovery, although the Council's Corporate Resilience Team held plans and procedures for different types of incidents, including a Corporate Emergency Response Plan and Business Continuity Strategy.</p> <p>It was understood that each Service within the Council was required to have an up to date Business Impact Analysis (BIA) – designed to assess and document the impact of an Information Security event or incident on the organisation and also gather the information needed to develop recovery strategies, and Business Continuity Plan – which is a playbook for resilience, including continuity plans in the context of</p>				
	<table border="1"> <thead> <tr> <th>Responsible Officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>David Wood</td> <td>31/12/2024</td> </tr> </tbody> </table>	Responsible Officer	Deadline	David Wood	31/12/2024	
Responsible Officer	Deadline					
David Wood	31/12/2024					

information security. However, it was noted in discussion that the BIA and BCP for the Croydon Digital Service (CDS) were not available and so not evidenced.

A full Business Continuity cycle was noted to be planned by the Corporate Resilience Team for Council Services later in 2024 to review BIA's and BCPs, including those of the CDS.

Risk

The absence of tailored Information Security response and recovery processes and procedures present risk of key stakeholders not being fully aware of their specific roles and responsibilities and being unprepared in the event of a cyber security incident. This leaves an organisation vulnerable to permanent data loss, unnecessary delay in returning to normal operations and increased potential of financial and reputational damage.

Control Area 2: Information Security Education and Training

Priority	Action by Management	Detailed Finding/Rationale - Issue 3
1	<p>The Information Security Manager will liaise with HR to understand the best process for ensuring appropriate engagement with policies and formal training is in place. The policy management platform (following some upgrades) can manage aspects of this task but may not be the appropriate corporate tool for all security training. Changes to the Oracle (HR) system may also assist but need to be fully understood. The intention will be to increase the quality and frequency (at least annually) of training to match today's risks, and to ensure there are proper consequences (e.g. appropriate disciplinary action) for non-completion.</p>	<p>Expected Control</p> <p>Personnel are aware of and fulfil their information security responsibilities and that this is communicated in a form that is relevant, accessible, and understandable to the intended reader. Recipients of the policies are required to acknowledge they understand and agree to comply with the policies where applicable.</p> <p>Finding/Issue</p> <p>Although there was a standard staff contract, which included a clause requiring new staff to read and abide by the "Acceptable Use of Email and Internet policy" (stated to be available on the intranet or from HR) there was no identifiable process in place to ensure that this policy, as well as other security policies, were read and understood by relevant personnel. Furthermore, available security policies were not easy to locate on the intranet.</p> <p>Similarly, the Standard Staff Contract provided for mandatory information security training for new staff during their probationary period and every three years thereafter. However, there was understood to be inconsistency in the implementation of the training although plans were underway to ensure regular and appropriate training on information security.</p> <p>Risk</p>
	<p>Responsible Officer</p> <p>Deadline</p>	

David Wood	31/01/2025	Lack of adequate information security awareness mechanisms increases the risk of personnel misusing the Council's systems and conducting inconsistent practice which could lead to unintentional disclosures of data or successful cyber-attacks.
------------	------------	---

Control Area 4: Technological Controls

Priority	Action by Management	Detailed Finding/Rationale - Issue 4
1	Ongoing tasks to measure and assess the effectiveness of controls in this area are gradually improving things, as will the new workstation rollouts and the enhanced use of the Intune systems for management of updates on these systems. These projects will be fully documented and leave us with detailed configurations and repeatable processes for maintenance, as well as contractual expectations on third parties to keep up to date with security of the new systems. The Information Security Manager now attends the service review	<p>Expected Control</p> <p>Appropriate technological controls are defined and documented to enhance information security and protect against cyber threats.</p> <p>Finding/Issue</p> <p>It was identified that none of the technical controls to protect the Council's information systems and networks had been uniformly defined and documented in line with the Annex A of ISO 27001.</p> <p>Technological controls identified, which required review and, as appropriate, definition, documentation, and uniform implementation, included the following:</p> <ul style="list-style-type: none"> • Configuration management • Access Control (privileged access rights, secure authentication, use of utility programs that might be capable of overriding system and application controls and installation of software)

	<p>meetings with key suppliers and has raised security issues with them as necessary. Server updates are still a concern, and some servers don't appear to be included in an update schedule. this is being escalated to the service delivery managers.</p>	<ul style="list-style-type: none"> • Secure development lifecycle (source code access, application security, secure system architecture and engineering principles, secure coding, outsourced development, separation of development, test, and production environments) • Capacity management • Data protection (Deletion and masking) • Data leakage prevention • Information back up • Logging • Monitoring activities • Network Security - major project in progress to refresh the entire network • Use of cryptography • Change Management
Responsible Officer	Deadline	
David Wood	31/01/2025	<p>Additionally, discussion noted that Littlefish provided services including anti-malware deployment and shared vulnerability management responsibilities with another managed service provider, Version 1. However, it was understood that service levels relating to the services were not adequately defined thereby limiting the Council's visibility over what was being implemented.</p> <p>Furthermore, the overall vulnerability management process was not defined or documented although plans on this were underway.</p> <p>Plans were in progress to remediate the gaps identified, including updating the Statements of Work (SOW) between the Council and service providers accordingly. Service levels in the SOW based on suitably defined and documented processes</p>

aligned with the relevant ISO 27001 controls would support the Council in ensuring best practices will be followed.

Risk

Processes and procedures deployed may not sufficiently protect information systems and networks against cyber threats without defined and documented controls which ensure appropriate alignment to best practices.

Control Area 1: Identity and Access Management

Priority	Action by Management	Detailed Finding/Rationale – Issue 5
2	<p>Information Security Manager is working with the HR team, notably on the Oracle project to ensure better management of people (staff and contractor) data, which will then be aligned to the access allocated to people. This should at the very least include integration into the processes for core systems managed by CDS, but we are intending it to include improved reporting of changes needed for all system administrators.</p> <p>This will be a significant change in the mindset of those who manage system access both within the business (owners) and CDS/Business (who often act as custodians). Specific reviews of access are now taking place to ensure admin rights are documented and minimised, and access (to core</p>	<p>Expected Control</p> <p>Information security and business requirements related to access control are determined to help ensure authorised access and prevent unauthorised access.</p> <p>Finding/Issue</p> <p>Although the AUP covers aspects of access control, discussion identified that various elements relating to access control required review to help ensure that appropriate and up to date processes, procedures and rules were defined, documented, and implemented. There were no comprehensively defined and documented identification and access management processes and procedures in place.</p> <p>For example, there were no defined processes for scheduled access reviews to ensure that all users (including users with elevated access rights) had the right level of access for their roles. Similarly, there were no effectively enforced processes for provisioning and de-provisioning users’ access to the Council’s corporate assets.</p> <p>Discussion noted that the absence of documented and implemented processes had led to a situation where access had not been revoked for some personnel who were no longer employed by the Council, and the access rights of personnel who had moved roles within the Council had not been changed, in some instances leading to the possibility of privilege creep. The Information Security Manager was collaborating with HR to correct the identified lapses.</p> <p>Risk</p>

	<p>systems) is removed when it is no longer required.</p> <p>Periodic reviews of access based on usage will remove people who are not using systems, and it is intended that managers will re-validate their staff's access periodically, with invalid access being removed from core systems.</p>	<p>A lack of effective identity and access management processes may lead to information and system breaches by either internal and external threat actors, privacy violations as well as financial and reputational damage.</p>
Responsible Officer	Deadline	
David Wood	31/01/2025	

Control Area 1: Supplier Relationships

Priority	Action by Management	Detailed Finding/Rationale - Issue 6
2	<p>An improved register of suppliers (first within CDS, but eventually organisation wide) will identify the suppliers in use, and they can then be risk assessed.</p> <p>Following this, a register of the risk-based due diligence and decisions made on suppliers can be put in place to demonstrate that security controls are appropriate for the supplier's role in the organisation.</p> <p>New suppliers are already going through a more robust process for checking and validation of their security credentials, and these are being recoded (for now) by the information security manager.</p>	<p>Expected Control</p> <p>Processes and procedures are defined and implemented to address information security risks associated with the use of supplier's products or services, to maintain an agreed level of information security in applicable supplier relationships and manage change in supplier information, security practices and service delivery.</p> <p>Finding/Issue</p> <p>There were not yet comprehensively defined and documented processes and procedures in place to manage information security requirements and mitigate any risks associated with suppliers' access to assets across the Council as a whole.</p> <p>Security requirements were generally addressed only when suppliers were engaged via the IT function, CDS. However, it was identified in discussion that within the CDS there was also still room for a more uniform and consistent approach to supplier due diligence enforced via defined processes.</p> <p>Furthermore, there were no established risk management processes for information security to be implemented for suppliers who engage with other Services outside of the CDS.</p> <p>Risk</p> <p>Information can be put at risk by suppliers without adequate information security management enforced within an organisation</p>
Responsible Officer	Deadline	

David Wood	31/12/2024	
------------	------------	--

Control Area 1: Asset Management (Operating Procedures)

Priority	Action by Management	Detailed Finding/Rationale - Issue 7				
2	Operating procedures for the Information Security function are under development and will form part of a wider documentation set as the function matures.	<p>Expected Control</p> <p>Operating procedures for information processing systems, services or infrastructure are documented and made available to personnel who need them to ensure the correct operation of the information processing facilities.</p> <p>Finding/Issue</p> <p>The Council had not identified whether there were relevant operating procedures for operational activities related to information security (information processing facilities) which should be documented and enforced. This potentially applied to arrangements including backup, management of audit trail and system log information and monitoring procedures such as capacity, performance, and security.</p>				
	<table border="1"> <thead> <tr> <th>Responsible Officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>David Wood</td> <td>31/1/2025</td> </tr> </tbody> </table>	Responsible Officer	Deadline	David Wood	31/1/2025	<p>Risk</p> <p>Where relevant operating procedures are not documented, this may jeopardise the correct and secure operation of information processing facilities.</p>
Responsible Officer	Deadline					
David Wood	31/1/2025					

Control Area 3: Physical Security

Priority	Action by Management	Detailed Finding/Rationale - Issue 8				
2	This is part of the Physical Access Policy, which is part of the reviewed policy set, and engagement is ongoing with the Facilities management team to implement this effectively.	<p>Expected Control</p> <p>The Council's organisation's tangible assets are protected from theft, damage, or unauthorised access.</p> <p>Finding/Issue</p> <p>Defined and documented processes and procedures related to physical access, environmental protection of information and secure facilities were not evidenced as a detailed analysis of these areas by the Information Security Manager, although expected had not yet commenced.</p> <p>It was noted that some physical controls had already been identified, which included demarcation of back-office sections from public areas and maintenance of manual logs to record guest access.</p> <p>The AUP addressed the use of USB sticks/key fobs. However, it was identified that processes and procedures around use of removable storage media, such as USB sticks, needed to be reviewed and appropriately defined to mitigate potential security risks. For example, the current security control leveraged via Bitlocker (Windows' security feature that provides encryption) would only prevent accidental but not deliberate disclosures.</p>				
	<table border="1"> <thead> <tr> <th>Responsible Officer</th> <th>Deadline</th> </tr> </thead> <tbody> <tr> <td>David Wood</td> <td>31/12/2024</td> </tr> </tbody> </table>	Responsible Officer	Deadline	David Wood	31/12/2024	<p>Furthermore, there were no defined and documented processes and procedures related to the provision of supporting utilities used to manage information systems to ensure continued equipment availability and integrity.</p> <p>Risk</p>
Responsible Officer	Deadline					
David Wood	31/12/2024					

Without robust physical security in place, there is potential for different risk exposure including, unauthorised access, data theft, insider threats. Also, without appropriately defined, documented, and enforced controls for removable media use, an organisation is exposed to risk of data breach.

AUDIT TERMS OF REFERENCE

ISO 27001 Annex A Gap Analysis

1. INTRODUCTION

- 1.1 London Borough of Croydon (the Council) is undergoing a period of change from both an organisational and cyber security perspective. It was noted during scoping discussions that a Security Policy framework has recently been developed to enhance cyber security practices and the organisation's security profile. The policies have been developed towards the Council's implementation and maintenance of an Information Security Management System (ISMS) which is aligned to the security control baselines in Annex A of the ISO 27001:2022 standard (ISO 27001).
- 1.2 ISO 27001 is an internationally recognised standard which prescribes baselines to manage information security risks.
- 1.3 Internal Audit has agreed to focus this audit on reviewing the Annex A of ISO 27001 against the controls in Croydon Council's security policy framework to ensure there is appropriate alignment.
- 1.4 This audit is part of the agreed Internal Audit Plan for 2023/24.

2. OBJECTIVES AND METHOD

- 2.1 The overall audit objective is to provide an objective independent opinion on the Annex A of ISO 27001 relative to Croydon Council's security policy framework.
- 2.2 The audit will consist of:
- High level documentation review.
 - Stakeholder validation workshops on the applicability of the Annex A of ISO 27001 to the Council's operations, and
 - Report on these accordingly.

3. SCOPE

- 3.1 This audit focused on the Information Security controls outlined in the Annex A of ISO 27001 against the Council's current security policy framework. The specific scope included the following areas and recommendations:

Control Areas/Risks	Issues Raised		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Organisational Controls	2	3	0
People Controls	1	0	0
Physical Controls	0	1	0

Control Areas/Risks	Issues Raised		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Technological controls	1	0	0
Total	4	4	0

3.2 The security policies reviewed was limited to the following:

- Acceptable Usage policy
- Information Security Policy
- Information Security Standard
- Workforce Data Protection Policy
- Data Protection Policy





3.3 The review was limited to the scope areas above and did not assess operating effectiveness of ISO27001 controls. Additionally, the review did not include:

- An analysis of compliance with clauses 4 to 10 of ISO 27001 which falls outside the scope of this review.
- Updating any policies, procedures, or documentation.
- An assessment of any IT areas outside of cyber security.
- Implementing, designing, or testing of any IT controls.
- An assessment of the implementation of the policies in scope or testing their effectiveness.

Definitions for Audit Opinions and Identified Issues

In order to assist management in using our reports:

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

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

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

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

Statement of Responsibility

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

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

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

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

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

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