Health Care Professional Council (HCPC)

Cyber Security

Internal Audit Report - Final

November 2025

Level of assurance:	
Design	Moderate
Effectiveness	Moderate

IDEAS | PEOPLE | TRUST

Contents

RESTRICTIONS OF USE

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

Distribution List		
For action	Anna Raftery	Head of Assurance and Compliance
	Nicole Jones	Improvement & Compliance Specialist
	Roy Dunn	Chief Information Security & Risk Officer
	Geoff Kirk	Head of IT and Digital
	Jason Roth	Infrastructure Architecture and Data Manager
For information	Audit Committee	

Report Status	
Auditor:	Alan Broadhead, Manager
Reviewers:	Dan Bonner, Director, Bill Mitchell, Responsible Individual
Fieldwork performed:	10 September to 12 September 2025
Closing meeting:	17 September 2025
Additional documents and queries:	24 September 2025
Draft report issued:	21 October 2025
Management responses received:	10 November 2025
Final report issued:	11 November 2025

Executive summary

Level of assurance: (see appendix I for definitions)		
Design	Moderate	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Moderate	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.

Definitions of findings (see appendix I)			# Of agreed actions
H	0		0
M	2		2
L	5		5
Total number of findings: 7			

Purpose

The purpose of this review was to assess HCPC's current implementation against NIST CSF 2.0 functions to validate the organisation's cyber security posture and identify areas for improvement. Specifically, this review evaluated the implementation progress of key procedures and arrangements regarding the following functions:

1. GOVERN - How cyber security risk management strategy and governance has been established.
2. IDENTIFY - Identifying and managing assets and cyber security risks.
3. PROTECT - Implementation of safeguards to manage cyber security risks.
4. DETECT - Finding and analysing cybers security attacks and compromises.
5. RESPOND – Responding to detected cyber security incidents.
6. RECOVER - Arrangements for restoring assets and operations affected by cyber security incidents.

Note that NIST CSF 2.0 functions have a direct mapping to NIST CSF 1.0 functions and referencing between them is straight forward. The primary difference between versions is the separation of the Govern function which previously formed part of the Identify function.

Background

As part of the agreed internal audit plan for 2025/26, as approved by the Audit and Risk Assurance Committee (ARAC), we have undertaken a key procedures review of cyber security.

The Health & Care Professions Council (HCPC) has undergone significant digital transformation over the past 18 months, implementing new business systems and modernising its technology infrastructure. While HCPC maintains robust cyber security assurance through ISO 27001 certification, Cyber Essentials Plus and PCI compliance, this review aimed to provide additional validation and to identify potential gaps not covered by existing frameworks.

The organisation has proactively implemented the NIST Cyber Security Framework (CSF) to provide comprehensive coverage of cyber security risks. This assessment will evaluate HCPC's progress against the NIST CSF 2.0 framework and provide strategic recommendations.

Summary of good practice

- ISO 27001:2022 and Cyber Essentials Plus certifications maintained
- Well-implemented Microsoft Defender E5 security stack
- Strong backup and disaster recovery arrangements
- Proactive NIST CSF implementation
- Robust patch management practices
- Effective network segmentation.

Executive summary

Our testing did not identify any concerns surrounding the controls in place to mitigate the following risks:

- ✓ Unclear accountability - Ambiguous roles and responsibilities leading to gaps in ownership.
- ✓ Asset inventory gaps - Unknown or unmanaged assets creating cyber security blind spots.
- ✓ Risk assessment limitations - Inaccurate risk prioritisation due to incomplete threat/ vulnerability analysis.
- ✓ Human error - Insufficient training leading to security policy violations and data breaches.
- ✓ Monitoring blind spots - Inadequate coverage of networks, systems, and user activities.
- ✓ Alert fatigue/noise - Poor event correlation leading to missed genuine threats.
- ✓ Limited threat detection - Reactive rather than proactive threat detection capabilities.
- ✓ Communication breakdowns - Poor coordination between internal teams and external stakeholders.
- ✓ Recovery time objectives - Extended downtime due to poor restoration planning and testing.
- ✓ Backup integrity issues - Compromised or untested backups failing during recovery operations.
- ✓ Business continuity gaps - Incomplete restoration of critical functions affecting organisational mission.

Summary of Medium significance findings

- IT staff have local administrative privileges on standard user accounts used for day-to-day activities, deviating from Cyber Essentials requirements and NIST CSF best practice for account separation. This presents elevated security risks as malware encountered during routine activities would execute with administrative rights, potentially enabling lateral movement across the network.
- HCPC do not have a formal process in place for the ongoing review of suppliers after initial onboarding. Without regular supplier reviews, HCPC faces the risk that suppliers may experience changes in their security posture, compliance status or business stability that could impact HCPC's operations and data security.

Conclusion

As part of our work we have identified seven findings, of which two were assessed as Medium and five as Low.

HCPC has strong cyber security arrangements in place, supported by ISO 27001 and Cyber Essentials Plus certifications. The organisation demonstrates a mature approach to information security with well-implemented technical controls including a comprehensive Microsoft Defender E5 security platform, robust backup and disaster recovery arrangements with regular testing, effective network segmentation and strong patch management practices. The proactive implementation of the NIST Cyber Security Framework through detailed system mapping demonstrates operational maturity and commitment to continuous improvement.

However, opportunities exist to strengthen arrangements further. The finding regarding IT staff using administrative privileges on standard user accounts presents elevated security risks and requires attention to meet Cyber Essentials requirements. The finding regarding supplier review requires attention due to the impact that key suppliers can have on an organisation if they are compromised. The five low-rated findings reflect improvement opportunities rather than fundamental security gaps, including documentation updates, policy alignment with current best practice (password expiry), finalising the incident response plan and the planned network infrastructure refresh.

As a result of our audit, we are able to provide Moderate assurance over the design and operational effectiveness of HCPC's cyber security arrangements.

Detailed Findings

Detailed Findings

Risk: Access control failures - Inadequate identity management.

Finding 1 - IT Staff Local Administrative Privileges	Type
In line with Cyber Essentials requirements and NIST CSF PROTECT function (PR.AA), administrative and standard user accounts should be separated. IT staff should use dedicated administrative accounts exclusively for performing administrative tasks such as installing software, making configuration changes and providing user support. Standard user accounts should be used for day-to-day activities including email, web browsing and document creation. This separation ensures that administrative privileges are not exposed to the risks associated with routine user activities. However, we identified that IT department members had local administrative privileges on their standard user accounts. The elevated privileges we identified for IT department members are being used for their day-to-day user activities including email, web browsing and general tasks, rather than being restricted to administrative activities only. We acknowledge there is a practical requirement for IT staff to perform support activities on other users' machines, where administrative privileges are necessary to provide remote assistance, however when IT staff perform routine activities such as web browsing or email access using accounts with local administrative privileges, any malware encountered during these activities would execute with administrative rights.	Design
Implication	**Significance**
The current configuration presents elevated security risks to the organisation as malware could disable security services, install unauthorised software, modify system configurations or spread laterally across the network.	Medium

Recommendation	Action owner	Management response	Completion date
1. HCPC should implement separate administrative accounts for IT staff to perform support and administrative functions. Standard approaches include creating dedicated administrative accounts (e.g. username_admin) that are only used for administrative tasks, while maintaining standard user accounts for daily activities. Alternatively, HCPC could evaluate implementing Privileged Identity Management (PIM) solutions that allow temporary elevation of privileges when required for specific administrative tasks, automatically de-escalating privileges after a defined period. This approach would maintain the operational flexibility needed for IT support while reducing security exposure. The solution chosen should balance operational requirements with security controls, ensuring IT support capabilities are maintained while reducing the attack surface presented by persistent elevated privileges.	Rick Welsby, IT Service Delivery Lead	User Account Control policies are already in place across all devices, and IT users can use separate domain admin credentials when elevated access is required. Local admin rights will be removed from standard IT user accounts. There is an issue for contact centre colleagues who currently need admin access for the telephony software, but a solution for this will be investigated once the Contact Centre phase 1 project has been successfully delivered.	31 March 2026

Detailed Findings

Risk: Inadequate governance oversight - Poor cyber security strategy integration with enterprise risk management.

Finding 2 - Ongoing Review of Suppliers			Type
HCPC do not have a formal process in place for the ongoing review of suppliers after initial onboarding. A formal supplier review process should be in place that includes regular periodic assessments of suppliers based on their risk profile and criticality to HCPC. This should align with NIST CSF Subcategories GV.SC-07 (risks posed by suppliers are monitored over the course of the relationship) and ISO 27001:2022 control A.15.2.1 (monitoring and review of supplier services). While the organisation has established supplier onboarding procedures that require ISO certification as a baseline requirement, no evidence was found of regular periodic reviews being conducted to assess suppliers' continued compliance with security requirements and to monitor changes in their risk profile.			Design
Implication			**Significance**
Without regular supplier reviews, HCPC faces the risk that suppliers may experience changes in their security posture, compliance status or business stability that could impact HCPC's operations and data security.			Medium
Recommendation	**Action owner**	**Management response**	**Completion date**
2. HCPC should develop a risk-based supplier review programme with different review frequencies based on supplier criticality and risk profile. For major suppliers like Microsoft, annual reviews could involve obtaining and reviewing SOC reports or equivalent third-party assurance reports. For smaller, higher-risk suppliers, more frequent reviews could be conducted potentially including direct engagement and updated risk assessments. The supplier review process could be integrated with the existing NIST framework implementation where key suppliers are already documented	Rick Welsby, IT Service Delivery Lead	A standard process will be added to the annual contract review and renewal process, requesting that suppliers provide HCPC with details of the maintenance of their security accreditations and of any independent tests they have undertaken. A more frequent process would not be viable given the scale of the HCPC and the number of suppliers involved.	31 March 2026

Detailed Findings

Risk: Incident response delays - Slow containment and escalation processes extending impact duration.

Finding 3 - Incident Response Plan Not Finalised			Type
HCPC's cyber security incident response plan is in draft status and had not been formally approved or implemented. During discussions with management, it was confirmed that the incident response document was still in draft format and had not been completed or formally adopted by the organisation. A comprehensive, formally approved cyber security incident response plan should be established, documented, and regularly tested. The plan should define clear roles, responsibilities, escalation procedures and recovery actions aligned with NIST CSF requirements under the RESPOND function (RS.MA - Incident Management). This is considered a critical document as per the National Cyber Security Centre for all organisations.			Design
Implication			**Significance**
Without an approved incident response plan, staff may be unclear about their roles and responsibilities during a security event, potentially leading to delayed response times, inadequate containment measures and inconsistent communication with stakeholders. This could result in extended incident duration and increased business impact.			Low
Recommendation	**Action owner**	**Management response**	**Completion date**
3. Management should complete and formally approve the cyber security incident response plan.	Roy Dunn, CISRO Jason Roth, IT Platforms & Architecture Lead	The document will be finalised and provided to the ISMS Board for sign-off.	31 March 2026

Detailed Findings

Risk: Inadequate governance oversight - Poor cyber security strategy integration with enterprise risk management.

Finding 4 - Policy Documentation Inconsistencies.			Type
During the review of HCPC's information security management system (ISMS) documentation, inconsistencies were identified between documented processes and current operational practices. Specifically, one policy referenced a two-month patching cycle when, in practice, the organisation implements a more stringent approach, patching critical and high-risk vulnerabilities within 14 days of release. Additionally, some policy documents contained outdated comments and references related to the transition to the ISO 27001:2022 standard that required updating to reflect current arrangements. Policy documentation should accurately reflect current operational practices and be regularly updated to remove outdated references and comments. Keeping documentation aligned with actual practices helps ensure clarity, supports effective communication and reinforces HCPC's commitment to maintaining high standards in information security management.			Design
Implication			**Significance**
While this finding represents a minor administrative issue rather than a substantive security gap, inconsistent policy documentation can lead to operational confusion and misalignment.			Low
Recommendation	**Action owner**	**Management response**	**Completion date**
4. HCPC should conduct a review of ISMS policy documentation to identify and update any inconsistencies between documented and actual practices.	Roy Dunn, CISRO	ISMS documentation is automatically assessed on an annual basis and documents will be reviewed and updated where necessary ahead of the next ISO27001 audit in March. Migration edits have been removed.	31 March 2026

Detailed Findings

Risk: Configuration drift - Inconsistent security configurations across platforms and environments.

Finding 5 - Legacy Network Equipment	Type
Wireless network equipment within HCPC's infrastructure was identified as being unsupported by the vendor; the Cisco 2504 Wireless Controller became obsolete on 30 April 2023 and the Wireless Access Points (Cisco Aironet 1600 Series) stopped being supported on 31 December 2021. This was identified during our review of the hardware asset register and discussions with IT management. Network equipment should be maintained within vendor support lifecycles with regular security updates and patches available. NIST CSF 2.0 subcategory PR.PS-02 requires that hardware is maintained, replaced and removed commensurate with risk. Cyber Essentials also requires that network device firmware receives regular security updates. We note the risk is significantly mitigated by HCPC's network segmentation approach where the Wi-Fi network is completely isolated from the corporate network with no bridge between them. The wireless network serves only as a guest network facilitating IoT devices and visitor access, requiring VPN authentication for any corporate resource access, hence the Low priority rating for this finding.	Design
Implication	**Significance**
Legacy wireless equipment operating beyond vendor support creates potential cybersecurity vulnerabilities as security patches and firmware updates are no longer available.	Low

Recommendations	Action owner	Management response	Completion date
5. HCPC should continue with their planned network infrastructure refresh project to replace the end-of-life wireless equipment. Regular monitoring of vendor support lifecycles should be implemented to provide advance warning of future end-of-support dates.	Jason Roth, IT Platforms & Architecture Lead	This work is part of the proposed Network Modernisation Project phase 2.	31 March 2027

Detailed Findings

Risk: Access control failures - Inadequate identity management.

Finding 6 - Password Policy Does Not Align with Current Best Practice	Type
HCPC requires users to change their passwords every 30 days. Current best practice guidance from NCSC and NIST CSF 2.0 recommends that organisations do not enforce regular password expiry, instead focusing on longer, more complex passwords combined with enhanced monitoring for compromised credentials. Where passwords are required to be changed frequently, this is likely to encourage the behaviour of staff choosing more predictable passwords. For example, users may adopt patterns such as incrementing numbers (e.g. Password01, Password02) or use simpler passwords that are easier to remember but less secure. It is noted that HCPC has multi-factor authentication successfully deployed across the organisation, which provides strong compensating controls and that consideration of this change has been discussed at the ISMS board level, demonstrating awareness of current best practice guidance, hence the Low priority rating of this finding.	Design
Implication	**Significance**
If users use less secure passwords then there is an increased risk of these being breached by a third party.	Low

Recommendations	Action owner	Management response	Completion date
6. HCPC should update their password policy to align with current NCSC and NIST guidance by removing the requirement for regular password expiry. The organisation should implement a policy requiring longer, more complex passwords (minimum 12 characters) that do not expire unless compromise is suspected. This approach should be combined with the existing MFA implementation and enhanced monitoring for compromised credentials through the current Microsoft security stack, which already provides risky sign-in detection and other advanced threat protection capabilities.	Roy Dunn, CISRO Rick Welsby, IT Service Delivery Lead	A review of HCPC's password management policies and options for adopting new practices will be provided to the ISMS Board for consideration and prioritisation against other cyber security activities. Refresher guidance on good passwords will be communicated to all employees.	31 March 2026

Detailed Findings

Risk: Threat intelligence issues - Poor understanding of current threat landscape and vulnerabilities.

Finding 7 - Root Certificate Authority Kept Online Despite Having Subordinate CAs	Type
During the review of the IT infrastructure, we identified that HCPC's root Certificate Authority (CA) server remained online and operational on the corporate domain, despite having subordinate Certificate Authorities in place for day-to-day certificate operations. This configuration deviates from established security best practice, which recommends that root CAs should be kept offline when subordinate CAs are available to handle routine certificate issuance. The organisation acknowledged that they had previously experienced connectivity issues when attempting to take the root CA offline and had made a pragmatic decision to keep it running continuously to avoid operational disruption and ensure consistent patching and maintenance. With subordinate Certificate Authorities already deployed, best practice dictates that the root CA should be kept offline as it is only required for infrequent administrative tasks such as issuing new subordinate CA certificates, certificate revocation list (CRL) updates or renewing the root certificate itself. The subordinate CAs should handle all routine certificate operations including user certificates, server certificates and other operational PKI (Public Key Infrastructure) requirements. The root CA should only be brought online for scheduled maintenance or when subordinate CA certificates require renewal or management. The root CA represents the highest trust anchor in the PKI hierarchy and keeping it online increases the attack surface without operational benefit. If compromised, an attacker could issue rogue certificates for any domain or service, potentially enabling man-in-the-middle attacks, impersonation of critical systems or complete PKI compromise. Since subordinate CAs can handle day-to-day operations, the online root CA creates additional risk without corresponding security benefits.	Design
Implication	**Significance**
Maintaining an online root CA when subordinate CAs are available presents unnecessary cybersecurity risks to the organisation.	Low

Recommendations	Action owner	Management response	Completion date
7. HCPC should investigate taking the root CA offline. The organisation should establish a scheduled maintenance approach where the root CA is only brought online for specific administrative tasks such as subordinate CA certificate renewal (typically required every 1-5 years depending on certificate validity periods). If immediate offline implementation presents technical challenges, HCPC should consider implementing compensating controls including network isolation of the root CA through dedicated VLANs and enhanced monitoring with alerting for any root CA access or certificate issuance.	Jason Roth, IT Platforms & Architecture Lead	The Root CA will be taken offline, and brought back online on a monthly basis for patching and maintenance.	31 March 2026

Appendices

Appendix I: Definitions

Level of assurance	Design of internal control framework		Operational effectiveness of controls	
	Findings from review	Design opinion	Findings from review	Effectiveness opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

Appendix II: Terms of reference

Extract from terms of reference		
Purpose		
The purpose of this high-level review was to assess HCPC's current implementation against NIST CSF 2.0 functions to validate the organisation's cyber security posture and identify areas for improvement.		
Scope area	**Key risks**	**Approach**
Govern	1. Inadequate governance oversight - Poor cyber security strategy integration with enterprise risk management. 2. Unclear accountability - Ambiguous roles and responsibilities leading to gaps in ownership.	Our approach will be to conduct interviews and walkthrough testing to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will: • Gain an understanding of the current procedures through discussions with key personnel, examining existing documentation and building on our knowledge obtained during scoping. • Evaluate the current state against the NIST CSF 2.0 subcategories and outcomes. • Review implementation progress and maturity. • Assess documentation and evidence supporting NIST framework adoption. • Identify areas where implementation could be strengthened. • Support any conclusions made and when developing the required recommendations.
Identify	1. Asset inventory gaps - Unknown or unmanaged assets creating cyber security blind spots. 2. Threat intelligence issues - Poor understanding of current threat landscape and vulnerabilities. 3. Risk assessment limitations - Inaccurate risk prioritisation due to incomplete threat/ vulnerability analysis.	
Protect	1. Access control failures - Inadequate identity management. 2. Configuration drift - Inconsistent security configurations across platforms and environments. 3. Human error - Insufficient training leading to security policy violations and data breaches.	
Detect	1. Monitoring blind spots - Inadequate coverage of networks, systems, and user activities. 2. Alert fatigue/noise - Poor event correlation leading to missed genuine threats. 3. Limited threat detection - Reactive rather than proactive threat detection capabilities.	
Respond	1. Incident response delays - Slow containment and escalation processes extending impact duration. 2. Communication breakdowns - Poor coordination between internal teams and external stakeholders.	
Recover	1. Recovery time objectives - Extended downtime due to poor restoration planning and testing. 2. Backup integrity issues - Compromised or untested backups failing during recovery operations. 3. Business continuity gaps - Incomplete restoration of critical functions affecting organisational mission.	

Appendix II: Terms of reference

Extract from terms of reference
Exclusions/ limitations of scope
The scope of the review was limited to the areas documented under the scope and approach. All other areas were considered outside of the scope of this review. We did not test the operating effectiveness of the functions and the associated controls.

Appendix III: Staff interviewed

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.		
Roy Dunn	Chief Information Security & Risk Officer	Executive sponsor
Geoff Kirk	Head of IT and Digital	Action owner
Jason Roth	Infrastructure Architecture and Data Manager	Action owner
Gerhard van Niekerk	IT Infrastructure Manager	Action owner
Michael Doe	IT Security Engineer	Action owner

Appendix IV: Responsibilities, limitations and conformance with the Global Internal Audit Standards

Management responsibilities

The Board is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The Board is responsible for ensuring the internal audit function has:

- The support of the Company's management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.
- The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Company.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the Company in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

Limitations

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

Conformance with the Global Internal Audit Standards

This engagement has been conducted in accordance with the Institute of Internal Auditors' Global Internal Audit Standards.

FOR MORE INFORMATION:

Bill Mitchell, Director, HIA
Bill.mitchell@bdo.co.uk

Disclaimer

This publication has been carefully prepared, but it has been written in general terms and should be seen as containing broad statements only. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication without obtaining specific professional advice. Please contact BDO LLP to discuss these matters in the context of your particular circumstances. BDO LLP, its partners, employees and agents do not accept or assume any responsibility or duty of care in respect of any use of or reliance on this publication, and will deny any liability for any loss arising from any action taken or not taken or decision made by anyone in reliance on this publication or any part of it. Any use of this publication or reliance on it for any purpose or in any context is therefore at your own risk, without any right of recourse against BDO LLP or any of its partners, employees or agents.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO member firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

The matters raised in this report are only those which came to our attention during our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

Copyright © 2025 BDO LLP. All rights reserved. Published in the UK.

www.bdo.co.uk