NHS Lothian

Backups & JML Review

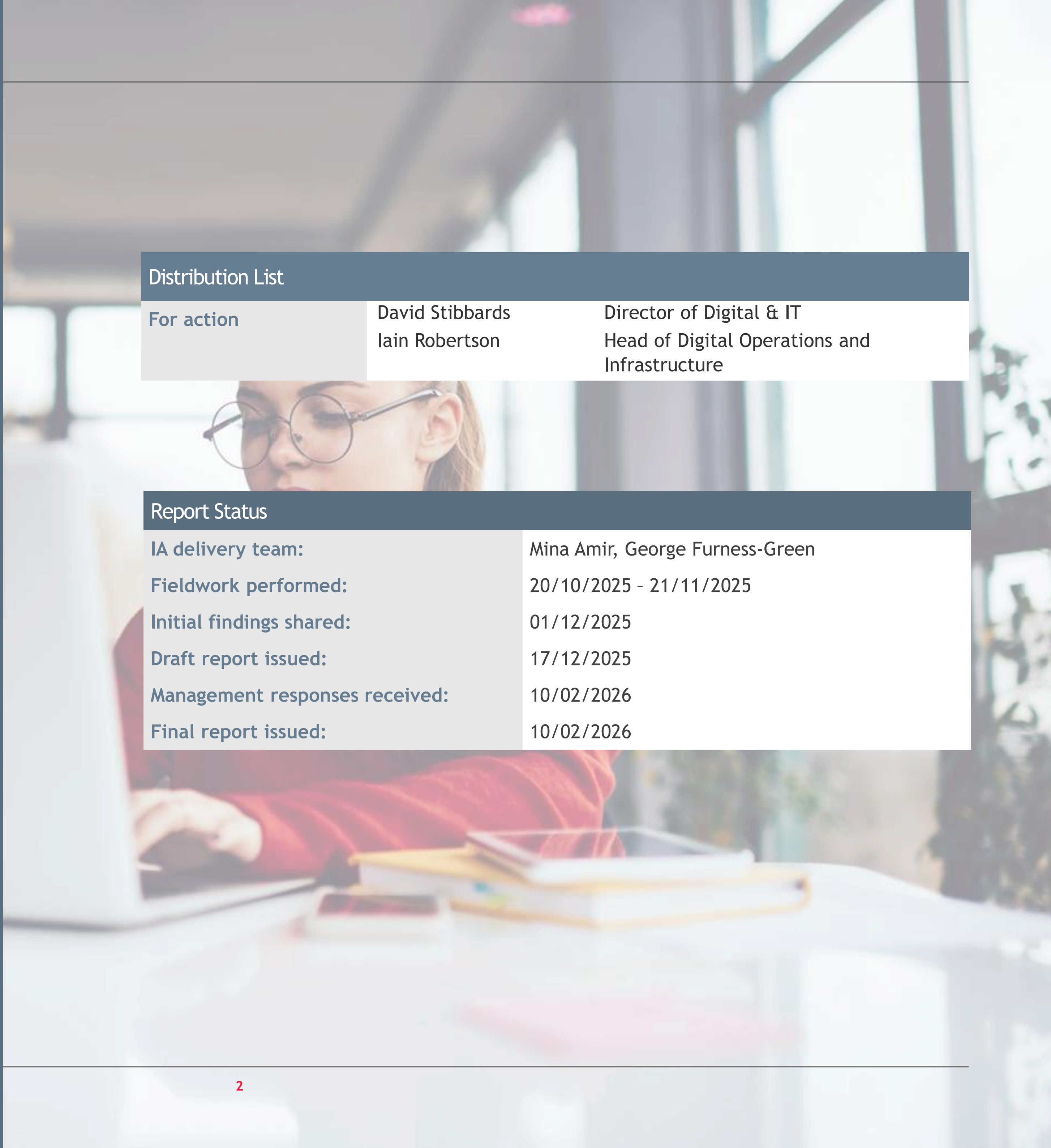
Internal Audit Report - Final

December 2025

Level of assurance:	
Design	Limited
Effectiveness	Limited

IDEAS | PEOPLE | TRUST

Contents



Distribution List		
For action	David Stibbards	Director of Digital & IT
	Iain Robertson	Head of Digital Operations and Infrastructure

Report Status	
IA delivery team:	Mina Amir, George Furness-Green
Fieldwork performed:	20/10/2025 – 21/11/2025
Initial findings shared:	01/12/2025
Draft report issued:	17/12/2025
Management responses received:	10/02/2026
Final report issued:	10/02/2026

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.

Executive Summary

Level of assurance: (see appendix II for definitions)		
Design	Limited	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	Limited	Non-compliance with key procedures and controls places the system objectives at risk.

Summary of findings		No. of Findings
H	🟥	2
M	🟨	2
L	🟩	2
Total number of findings		6

Purpose

The review aimed to evaluate the effectiveness and robustness of the NHS Lothian's backup and JML processes, identifying any weaknesses or areas for improvement that could affect data security and operational efficiency.

Background

It was agreed as part of the 2025-26 Internal Audit Plan that Internal Audit would conduct a review of a review of Backups and JML (Joiners, Movers, Leavers) at NHS Lothian (NHSL) pertaining to Active Directory (AD).

This audit is essential to ensure operational efficiency and safeguard sensitive data within the organisation. The review of backup processes is vital to protect against data loss and ensure business continuity.

NHSL recently updated its backup solution, which has not yet undergone an audit. This presents a valuable opportunity to assess the new system. The change was prompted by the expiration of a previous contract, leading NHSL to explore market alternatives. The new solution enhances backup capabilities, including the ability to perform immutable backups. The system now backs up more data and utilises opposite sites for redundancy. This change in product and increased backup capacity is a key area for review during the audit.

By examining current backup procedures, we aimed to identify any vulnerabilities and recommend improvements to enhance data security and reliability.

The JML process is a key area that impacts operational efficiency. Managing the lifecycle of employees from their onboarding to role changes and eventual departure requires robust systems to ensure access rights are appropriately granted and revoked. This audit assessed the effectiveness of current JML procedures, identifying areas where improvements can be made to streamline operations and reduce the risk of unauthorised access to sensitive information.

By addressing these critical areas, we aim to support NHS Lothian in achieving its strategic objectives and enhancing its overall service quality.

Conclusion

The audit noted several good practices, including:

- The backup solution has been updated to streamline processes, including offsite safeguards for disaster recovery.
- Backups are monitored daily, and failures are rectified promptly.
- Active Directory (AD) provisioning is centrally managed with robust approval and least privilege controls.

Notwithstanding the areas of good practice, we have raised six findings, two of high significance, two of medium significance and two of low significance. The high and medium findings relate to:

- A process is not in place for handling employee role changes (movers), increasing the risk of compounded inappropriate access.
- Access for leavers is not revoked in a timely manner, increasing the risk of unauthorised access to systems and sensitive data following employee termination.
- Incomplete assurance over backup coverage for critical systems, including high-risk IT services, increasing the risk of data loss and prolonged service disruption.
- Outdated access management SOPs (JML, O365 Account Creation & Digital System & Domain Administrator Accounts) were identified, increasing the risk that policies and procedures are misaligned with current processes over time.

We have issued an overall assurance opinion of *limited* due to the number of design gaps identified as part of this review.

Detailed Findings

Detailed Findings

Risk (as per ToR): Inadequate user access management policies and procedures for joiners, movers, and leavers could lead to unauthorised access, data breaches, and compliance issues, compromising organisational security and integrity (Movers - Active Directory (AD) access changes).

Finding 1 - Absence of embedded Movers Process for Active Directory	Type
A defined and embedded process for handling employee role changes (movers) is not in place. IT is not consistently notified when employees move roles, and access changes are typically addressed only through additional access requests. As a result, employees who change roles may retain access to systems associated with their previous position and be assigned additional privileges creating access conflicts. Without an embedded process, employees may accumulate excessive or inappropriate access rights, increasing the risk of: Security breaches (e.g., unauthorised access to sensitive data or systems), compliance failures with regulatory requirements (e.g., GDPR, ISO 27001) and privilege escalation, which could be exploited for fraud or data misuse.	Design

Implication	Significance
Employees who change roles may retain unnecessary or excessive access rights, increasing the risk of unauthorised access, data breaches, and non-compliance with security policies.	High

Recommendations	Action owner	Management response	Completion date
Management should establish a formal, documented process for handling employee role changes within the Joiners, Movers, and Leavers (JML) framework. This process should include: 1. Mandatory notifications to IT when an employee changes roles. 2. Automated or scheduled access reviews to revoke permissions no longer required and grant only those necessary for the new role. 3. Clear ownership and accountability for initiating and approving access changes (e.g., HR and IT collaboration). 4. Integration with existing JML processes and leverage automation tools (e.g., identity management systems) to minimise manual oversight and reduce errors.	Head of HR Systems	A workgroup has been established with key people in HR and Digital to review and revise the JML Process. This is a significant piece of work, but the group has been established with a clear terms of reference and membership. The audit items identified will be incorporated into this workstream.	December 2026

Detailed Findings

Risk (as per ToR): **Poorly designed JML processes could result in ineffective user access management, leading to security vulnerabilities, unauthorised access, and potential data breaches, impacting organisational security and compliance (Leavers - delayed account deactivation).**

Finding 2 - Delayed Deactivation of Leaver Accounts	Type
IT currently relies on a monthly HR leaver listing to identify employees who have left the organisation. This process means that individuals who have exited the business may retain access to critical systems for up to one month after their termination date. Our sample testing revealed significant gaps in timely account deactivation: • 6 out of 10 leaver accounts tested were not deactivated within one month of the employee's HR termination date. • In one case, an Active Directory (AD) account for a leaver remained active at the time of review, despite the employee leaving on 31 July 2025. This indicates that the current process lacks real-time notifications and automated controls, creating a prolonged window where former employees can access sensitive systems and data. Such delays increase the risk of unauthorised access, data breaches, and non-compliance with security standards.	Design & Effectiveness
Implication	**Significance**
Former employees retaining active accounts can lead to security breaches, data loss, and compliance violations, exposing the organisation to financial and reputational damage.	High

Recommendations	Action owner	Management response	Completion date
Management should implement a formal process to ensure timely removal of system access for leavers, including: 1. Automated notifications to IT when termination dates are confirmed. 2. Defined timelines for deactivation (e.g., within 24-48 hours of leaving). 3. Periodic access reviews to identify and remove any active accounts for former employees. 4. Integration of HR systems with Active Directory or IAM tools to minimize manual steps and reduce risk. 5. Review existing automated scripts for AD account removal to ensure functionality and coverage.	Head of HR Systems Head of Digital Ops	1-4. A workgroup has been established with key people in HR and Digital to review and revise the JML Process. This is a significant piece of work, but the group has been established with a clear terms of reference and membership. The audit items identified will be incorporated into this workstream. 5. The removal scripts will be modified as suggested.	December 2026 June 2026

Detailed Findings

Risk (as per ToR): Poor management of backup procedures, IT systems, recovery objectives, and third-party services could lead to non-compliance, disruptions, vulnerabilities, and data loss (Backup coverage - completeness across critical systems).

Finding 3 - Incomplete Assurance over Backup Coverage for Critical IT Systems and Services	Type
NHS Lothian has recently implemented backup processes for production servers; however, there is insufficient assurance that backup coverage extends to all critical IT architecture, including high-risk IT systems and services and non-standard platforms. The Backup Standard Operating Procedure (SOP) primarily highlights production servers and does not clearly confirm that all critical systems, such as authentication services, domain controllers and critical application servers, are consistently included within the backup processes. In addition, the SOP does not explicitly address backup coverage for unsupported operating systems or legacy platforms that may fall outside standard backup configurations. As a result, there is limited assurance that backup coverage is complete, consistently applied and aligned with business continuity and disaster recovery requirements. Without clear confirmation and validation of backup scope, there is a risk that critical systems may be unintentionally excluded. This increase the risk that in the event of a system failure, cyber incident or disaster, the organisation may be unable to fully restore critical systems and services in a timely manner, potentially resulting in data loss and prolonged service disruption.	Design
Implication	**Significance**
Incomplete assurance over backup coverage could result in incomplete recovery during outages or disasters, exposing the organisation to operational disruption, data loss, financial loss, and compliance breaches.	Medium

Recommendations	Action owner	Management response	Completion date
Management should enhance assurance over backup coverage to confirm that all critical architecture are included within the existing backup processes. This should include: 1. Defining a complete inventory of critical systems and services requiring backup coverage. 2. Confirming and documenting backup coverage against the defined inventory, including any exclusions. 3. Validating backup completeness and recoverability through periodic testing and to ensure alignment with BC/DR requirements. 4. Updating supporting documentation (e.g. backup SOP) to reflect the confirmed backup scope and validation/testing activities.	Head of Digital Operations	1. Such an inventory is neither practical nor required. All request for new applications undergo a design, and that includes stating how they are backed up. As a result no system can be deployed without it being clear how it is backed up. 2. The backup schedule shows all systems backed up and errors, which are then acted upon. This is not a practical solution with hundreds of databases and thousands of files backed up daily.	N/A - Risk accepted N/A - Risk accepted

Detailed Findings

Risk (as per ToR): Poor management of backup procedures, IT systems, recovery objectives, and third-party services could lead to non-compliance, disruptions, vulnerabilities, and data loss (Backup coverage - completeness across critical systems).

Recommendations	Action owner	Management response	Completion date
	Head of Digital Operations	3. The current policy states tests are to be performed twice a year if no restores are performed to support normal business. This will be revised. 4. The backup SOP will be revised	June 2026 June 2026

Detailed Findings

Risk (as per ToR): **Inadequate user access management policies and procedures for joiners, movers, and leavers could lead to unauthorised access, data breaches, and compliance issues, compromising organisational security and integrity (Access management SOP governance – review and maintenance).**

<table>
<tr><th colspan="3">Finding 4 - Weaknesses in Access Management SOP Governance</th><th>Type</th></tr>
<tr><td colspan="3">During the review, it was noted that key access management Standard Operating Procedures (SOPs) documents had not been reviewed or updated in line within the defined review cycle (annually). While joiner and leavers processes are documented, weaknesses in SOP governance reduces assurance that procedures remain current, complete and aligned to how access management process are intended to operate.

The following SOPs had not been reviewed within the expected review schedule:

• SOP JML (last reviewed in 2023)
• SOP O365 Account Creation (last reviewed in 2023)
• Digital System & Domain Administrator Accounts (last reviewed in August 2024)

Weaknesses in SOP governance increases the risk that access management procedures become outdated or misaligned over time, which could lead to inconsistent execution, control gaps, or reliance on informal practices, particularly as processes or systems change.</td><td>Design</td></tr>
<tr><th colspan="3">Implication</th><th>Significance</th></tr>
<tr><td colspan="3">Inadequate governance over access management SOPs can lead to inconsistent processes, operational inefficiencies, and security weaknesses, exposing the organisation to compliance failures and potential data breaches.</td><td>Medium</td></tr>
<tr><th>Recommendations</th><th>Action owner</th><th>Management response</th><th>Completion date</th></tr>
<tr><td>Management should implement strengthen governance over access management SOPs to ensure procedures remain current and fit for purpose. This should include:

1. Ensuring SOPs are reviewed and updated in-line with the defined review cycle.
2. Assigning clear ownership for maintaining access management documentation.
3. Documenting approvals and version controls for all SOP changes.
4. Where possible, implement a centralised policy management system or automation tools to reduce the risk of SOPs becoming outdated.</td><td>Head of Digital Ops</td><td>1 2,3 Some of the SOP's presented were sub department SOP's and were indeed out of date, and in need of review.
All Sub department SOP's will be reviewed and revised.
4. Processes will be established for review & revision. The team will look at potential solutions as suggested.</td><td>June 2026</td></tr>
</table>

Detailed Findings

Risk (as per ToR): Poor management of backup procedures, IT systems, recovery objectives, and third-party services could lead to non-compliance, disruptions, vulnerabilities, and data loss (RTO/RPO documentation - alignment to BIA/BCP).

Finding 5 - Lack of Explicit Documentation for Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) within backup SOP	Type
The current SOP references RTO and RPO values conceptually but does not explicitly document them or provide direct linkage to supporting documents such as the Business Impact Analysis (BIA) or Business Continuity Plan (BCP). While the SOP mentions that these values are defined elsewhere, they are not cross-referenced or included for clarity and ease of reference. This lack of explicit documentation creates ambiguity for teams responsible for disaster recovery and business continuity, as they may not have immediate access to critical recovery objectives during an incident. It also increases the risk of misalignment between SOPs and organisational resilience requirements.	Design
Implication	**Significance**
Unclear or missing RTO/RPO documentation can hinder effective disaster recovery planning and execution, potentially leading to prolonged downtime and non-compliance with resilience requirements.	Low

Recommendations	Action owner	Management response	Completion date
Management should ensure that RTO and RPO values are explicitly documented within the SOP or clearly cross-referenced to relevant continuity documents. This should include: 1. Direct inclusion or linkage of defined RTO/RPO values in the SOP for clarity. 2. Version control and alignment checks to confirm consistency between SOP, BIA, and BCP. 3. Periodic reviews to ensure documented objectives remain aligned with business continuity requirements and regulatory expectations.	Head of Digital Ops	1. The RTO already exists in the policy. The RPO will be added 2. The SOP's are formally reviewed every year. This feedback will be incorporated in the 2026 revision 3. Whilst a process for annual review of SOP's exists, there is no log of which SOP's are reviewed. Going forward a log of these approvals will be recorded.	June 2026 November 2026 June 2026

Detailed Findings

Risk (as per ToR): Poor management of backup procedures, IT systems, recovery objectives, and third-party services could lead to non-compliance, disruptions, vulnerabilities, and data loss (Third-party backup responsibilities - roles and SLAs).

Finding 6 - Lack of Explict Reference to Third-Party Backup Responsibilities within backup SOP	Type
The backup SOP mentions infrastructure components such as Dell Powescales and Libre NMS, and backup responsibilities are assigned internally. In addition, service level agreements (SLAs) and contractual arrangement with third-party provider's supporting backup and restore activities were reviewed as part of this review. However, the backup SOP document does not explicitly reference these third-party arrangements, including roles, responsibilities or relevant SLAs for backup and restore processes. As a result, the SOP does not provide a complete view of accountability across internal teams and external providers. This absence of explicit references to third-party roles and SLAs within the backup SOP creates ambiguity around accountability by external providers. In the event of a failure or service disruption, this could delay escalation, resolution, or recovery activities.	Design
Implication	Significance
Unclear documentation of third-party responsibilities within backup procedures may result in delays or inefficiencies during incident response or recovery activities.	Low

Recommendations	Action owner	Management response	Completion date
Management should update the backup SOP to reflect the roles and responsibilities for both monitoring the daily backup log and for actions required from this log (incl. any third-party support): This should include: 1. Clear identification of roles and responsibilities (of internal and external parties) for monitoring the backup log. 2. Identification of roles for actions identified in the backup log.	Head of Digital Ops	1 & 2. The backup SOP will be updated to clearly define roles, responsibilities and monitoring frequency for the daily backup log and to specify who is responsible for taking action on any issues identified. This will be incorporated as part of the next scheduled SOP review.	November 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.
Not Compliant	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

Scope area	Procedure title	Key risks	Approach
Backup and Restore	Documentation Review	Poor management of backup procedures, IT systems, recovery objectives, and third-party services could lead to non-compliance, disruptions, vulnerabilities, and data loss.	• Obtain and review the organisation's backup and restore policies and procedures. • Confirm that all critical architecture (including high-risk IT systems and services) is adequately addressed. • Ensure that Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are documented and align with business requirements. • Verify that third-party and outsourced service providers are appropriately incorporated within these policies.
	Changes to the Backup Scheduler	Unauthorised or poorly documented changes to backup schedules or storage locations could lead to data loss, non-compliance, and operational inefficiencies, compromising the organisation's ability to recover effectively.	• Examine change management processes to confirm that any updates to backup schedules or storage locations are properly authorised and documented.
	Configuration Review	Non-compliance of backup configurations with documented policies and procedures could lead to data protection failures and hinder recovery efforts, impacting business continuity.	• Verify that current backup configurations comply with the documented policies and procedures
	Sample Testing of Backup Logs	Inadequate adherence to backup policies and unresolved backup failures could compromise data integrity and recovery processes, affecting the organisation's ability to maintain business continuity.	• Conduct a sample test of backup logs to confirm proper adherence to backup policies. • Verify that any backup failures have been adequately investigated and resolved.
	Backup Restore Testing	Insufficient backup restore testing and lack of alignment with industry best practices could lead to ineffective recovery processes, jeopardising data integrity and business continuity.	• Determine when the most recent backup restore testing was performed. • Conduct a desktop review of the relevant documentation, assessing scope, methodology, and outcomes. • Compare these elements against industry best practices (e.g., frequency, depth of testing, inclusion of critical systems). • Identify any necessary improvements in test planning, execution, and follow-up actions.

Appendix II: Terms of reference

Scope area	Procedure Title	Key risks	Approach
Joiners, Movers, Leavers (JML)	Policy and Procedure Review	Inadequate user access management policies and procedures for joiners, movers, and leavers could lead to unauthorised access, data breaches, and compliance issues, compromising organisational security and integrity.	• Obtain and review policies and procedures relating to user access management, including Joiner/Mover/Leaver (JML) processes.
	Design Assessment	Poorly designed JML processes could result in ineffective user access management, leading to security vulnerabilities, unauthorised access, and potential data breaches, impacting organisational security and compliance.	• Assess the design of these processes by examining documented evidence and interviewing control owners responsible for their operation.
	Sample Testing	Failure to accurately manage user access for joiners, movers, and leavers could lead to unauthorised access, data breaches, and non-compliance with security policies, affecting the organisation's security posture and operational integrity.	• Perform sample testing of joiners, movers, and leavers, in Azure AD and AtoS Backup tool. • Confirm that each user's access is appropriately added, modified, or removed in line with the documented JML procedures.

Exclusions/limitations of scope

The scope of the review is limited to the areas documented under the scope and approach. All other areas are considered outside of the scope of this review. Our review will provide assurance over the below two systems in scope only:

1. Azure AD
2. AtoS (Backup)

Where sample testing is undertaken, our findings and conclusions will be limited to the sample tested only. Please note that there is a risk that our findings and conclusions based on the sample may differ from the findings and conclusions we would reach if we tested the entire population from which the sample is taken.

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.		
David Stibbards	Director of Digital and IT	Key Contact
Iain Roberston	Head of Digital Operations and Infrastructure	Key Contact
Derek Gibson	Head of IT Operations	Interviewee
Paul Bryan	IT Operations Manager	Interviewee

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:

Sandi Dosanjh
Digital Partner
+44 (0) 784 156 9636
sandi.dosanjh@bdo.co.uk

Claire Robertson
Head of Risk Advisory Services (Scotland)
+44 (0) 758 323 7579
Claire.Robertson@bdo.co.uk

Freedom of Information

In the event you are required to disclose any information contained in this report by virtue of the Freedom of Information Act 2000 (“the Act”), you must notify BDO LLP promptly prior to any disclosure. You agree to pay due regard to any representations which BDO LLP makes in connection with such disclosure, and you shall apply any relevant exemptions which may exist under the Act. If, following consultation with BDO LLP, you disclose this report in whole or in part, you shall ensure that any disclaimer which BDO LLP has included, or may subsequently wish to include, is reproduced in full in any copies.

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.

www.bdo.co.uk