ICT Audit

FINAL

Southway Housing Trust

ICT Review of IT Access Controls

2023/24

November 2023

Executive Summary

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

Risk 27 - Due to lack of formally adopted process for managing staff Joiners, Movers and Leavers, we are unable to implement adequate controls to maintain network security, resulting in potential data breach and potential litigation and damage to reputation

SCOPE

The review considered the processes in place for granting access rights to the key systems including access for temporary staff, staff who have been promoted or moved jobs and staff leaving the Trust.

KEY STRATEGIC FINDINGS

Policy and procedures require updating to clearly define the process and controls, as planned.

Testing did not identify any inappropriately active user accounts.

A formal and frequent user access reconciliation is required to provide more robust assurance that user access controls remain effective and any anomalies are identified and corrected.

The current Starters, Movers and Leavers Procedure involves processing requests for HR and ICT in parallel, which introduces the risk of inconsistencies.

GOOD PRACTICE IDENTIFIED

The ICT ticketing system provides an audit trail, broken down by system, of the process for the establishment, alteration and deletion of user access.

ACTION POINTS

Urgent	Important	Routine	Operational
0	2	1	0

Assurance - Key Findings and Management Action Plan (MAP)

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Directed	The ICT Team reconcile active AD user accounts against current employees on an annual basis. A more frequent and formal reconciliation is required to provide more robust assurance that user access controls remain effective.	A formal and frequent user access reconciliation is required to provide more robust assurance that user access controls remain effective and any anomalies are identified and corrected.	2	*ICT will implement a quarterly reconciliation between the HR solution and the active Directory user list.* *It will be marked as a recurring ticket in the helpdesk system for audit purposes.* *As HR are now using the same solution an automatic ticket for HR can be created at the same time.*	*30/11/23*	*Ian Hardingham (Head of ICT)*
3	Directed	The current Starters, Movers and Leavers Procedure requires managers to provide written notification to the HR team via email and to Log an ICT Service Ticket with the New Starter Details. Processing requests in parallel introduces the risk of inconsistencies. As the procedure states that HR have the responsibility to "notify the ICT department of impending additions and changes to staffing as soon as they become aware of such situations so that relevant computer security amendments and updates can be scheduled in a timely fashion to ensure all access is properly authorised and appropriate.", the HR department do not have the required oversight and approval of manager's requests.	The current Starters, Movers and Leavers Procedure be reviewed to confirm that HR have the appropriate level of oversight for the creation and changes to user accounts.	2	*HR are taking the lead on the Starters, Movers and Leavers process. ICT will be on the new improved process to receive notification directly from HR with the details of the new starter.* *As HR are using the same solution as the ICT Helpdesk, we can link tickets to create automation supporting the efficiency of the process.*	*31/12/23*	*Nigel Shaw (Head of HR)*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	A Digital Workplace programme of change is currently taking place, which involves considerable changes to infrastructure with corresponding future changes to process. The current policies and procedures are, therefore, applicable to the current arrangements but won't be once the infrastructure changes. It has been agreed with Board that the documentation will be refreshed and renewed following the go live planned for early November. Affected policies and procedures include: • Information Security Policy (COR-POL-25) • ICT Network Security Policy (ICT-POL-04).	Policies and procedures be reviewed and updated following the completion of the Digital Workplace programme of change as planned.	3	*The Information Security Policy (COR-POL-25) and the ICT Network Security Policy (ICT-POL-04) are both scheduled for review the end of Q3 (Dec) into Q4 2023-24 following the go live of the new Infrastructure.*	*31/03/24*	*Ian Hardingham (Head of ICT)*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Operational - Effectiveness Matter (OEM) Action Plan

Ref	Risk Area	Finding	Suggested Action	Management Comments
No Operational Effectiveness Matters were identified.				

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Findings

Directed Risk:

Failure to properly direct the service to ensure compliance with the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
GF	**Governance Framework**	There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation.	Partially in place	1, & 2	-
RM	**Risk Mitigation**	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	In place	-	-
C	**Compliance**	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Partially in place	3	-

Other Findings

A Starters, Movers and Leavers Procedure is in place to provide a framework for the management of user access permissions, specifically actions that must be taken when staff are:

- Starting employment with the Company;
- Moving between departments or changing job roles in current departments; and
- Leaving employment with the Company.

Each request must be made via the ICT Service Desk ticketing system, which, under the category of Starters and Leavers, allows the selection of:

- Changes Users Job or Permissions;
- Leavers Request; and
- New Starter Request.

This process provides a structure to employee management and allows an audit trail.

Other Findings

The New Starters Procedure requires:

Responsible line managers are to provide written notification to the HR team via email and to Log an ICT Service Ticket with the New Starter Details, which are detailed in Appendix A and must include the following information:

- Employee Name;
- Employee Department;
- Employee – Software Required; and
- Employee Start Date;
- Employee Job Title for the new employee;
- Officer undertaking similar duties (if relevant).
- Employee Line Manager;
- Employee – Equipment Required;

Appendix B lists the systems that are affected by changes to staffing and actions that ICT Service must perform to maintain security:

Microsoft Active Directory	• Relevant security groups updated.
	  ◦ Add new groups
	  ◦ Remove from unneeded groups.
	• Job Description, Extension No, Department.
	• Update OU.

Web Help Desk	• Update the IT asset register.
Microsoft Exchange	• Update email distribution group memberships.
Capita OPENHousing	• Update relevant security groups to reflect role changes • Set leavers accounts to “inactive”.
Total Mobile	• Set leavers accounts to “inactive”.
Devices	• Mobile Devices – Wipe and return to default state via MDM. • Laptops – Wipe and rebuild with fresh image. • PC’s – Wipe and rebuild with new image.

For Leavers, a Service Desk ticket must be raised with the Employee Name and Employee Leaving Date populated.

For Movers, a Change Users Job or Permissions must be raised as a ticket to the Service Desk which requires the same details as for a new starter.

Other Findings

The Trust has identified risks associated with the process which include:

- Risk 8 - Due to poor management controls, requests made by business service lines for changes in core Housing Systems allow staff to generate business commitments exceeding their level of authority, resulting in high value unauthorised commitments and / or potential disputes, claims, litigation.
- Risk 13 - Due to 3rd Party Support providers having control over their password setting and having fixed passwords that do not require regular changing, supplier accounts exist with simple well-known passwords, leading to potential weakness in system security, unauthorised access and litigation or regulatory compliance issues.
- Risk 18 - Due the implementation of some user accounts with fixed passwords, logon details could be known by persons leaving the Company, leading to potential security breach and regulatory compliance issues.
- Risk 27 - Due to lack of formally adopted process for managing staff Joiners, Movers and Leavers, we are unable to implement adequate controls to maintain network security, resulting in potential data breach and potential litigation and damage to reputation.
- Risk 38 - Due to Security Access in the core housing system being poorly configured during initial system implementation and poorly managed during starter, mover and leaver processes, access levels for some members of staff are inappropriate, resulting in potential inappropriate access to confidential data, data corruption and potential interest from regulating bodies.
- Risk 51 - Due to ICT Admin accounts having extensive access to network resources, an IT member could make a deliberate or inadvertent system change which negatively impacts system configurations, system stability, system availability or compromises business data, leading to significant impact to business operations and/or regulatory implications.

This provides assurance that the risks are recognised, managed and monitored.

For the purposes of testing, the following resources were provided:

- An exported spreadsheet of all user network accounts on Active Directory (AD);
- Lists of all starters, leavers and movers since January 1st 2023;
- A list of Current Employees and Job Titles, and Agency staff from HR; and
- An export of tickets raised on the ICT Service desk of type Starters and Leavers.

The AD user network account list was filtered to show employees only and a comparison made to the HR records. Reconciliation of AD users against current employees identified five employees which closely matched AD users. HR confirmed that four of the five were given names on iTrent HR System and preferred name on AD. It is noted that iTrent also holds the preferred names.

Five accounts were found to be present on AD but not iTrent. Upon investigation, HR confirmed that they were consultants who need system access but don't necessarily need adding to iTrent.

A further three accounts on AD were on the new starters list but not on HR's current employee list. HR confirmed that these are new starters who are due to start. ICT will have created a profile for them but they haven't been added to HR system as they haven't started.

A final discrepancy was a user who is on the leavers list but is still active. HR confirmed this user is a leaver but works occasional days for the Association, however, in HR terms is a leaver so not on the iTrent system.

Delivery Risk:

Failure to deliver the service in an effective manner which meets the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
PM	Performance Monitoring	There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner.	In place	-	-
S	Sustainability	The impact on the organisation's sustainability agenda has been considered.	Out of scope	-	-
R	Resilience	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	In place	-	-

Other Findings

The ICT ticketing system provides an audit trail, broken down by system, of the process for the establishment, alteration and deletion of user access.

EXPLANATORY INFORMATION

Appendix A

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review, and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Effectiveness of arrangements

3. The definitions of the effectiveness of arrangements are set out below. These are based solely upon the audit work performed, assume business as usual, and do not necessarily cover management override or exceptional circumstances.

In place	The control arrangements in place mitigate the risk from arising.
Partially in place	The control arrangements in place only partially mitigate the risk from arising.
Not in place	The control arrangements in place do not effectively mitigate the risk from arising.

Assurance Assessment

4. The definitions of the assurance assessments are:

Substantial Assurance	There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved.
Reasonable Assurance	The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved.
Limited Assurance	The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved.
No Assurance	There is a fundamental breakdown or absence of core internal controls requiring immediate action.

Acknowledgement

5. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

6. The table below sets out the history of this report.

Stage	Issued	Response Received
Audit Planning Memorandum:	15th May 2023	15th May 2023
Draft Report:	9th October 2023	2nd November 2023
Final Report:	13th November 2023	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Southway Housing Trust		
Review:	IT Access Controls		
Type of Review:	Assurance	**Audit Lead:**	Simon Butterfield

Outline scope (per Annual Plan):	The review considers the processes in place for granting access rights to the key systems including access for temporary staff, staff who have been promoted or moved jobs and staff leaving the Trust.
Detailed scope will consider:	The review will set out to provide assurance to the Audit Committee that the Trust has appropriate IT access controls processes in place. • The policy and procedures are up-to-date and clearly define the process and controls. • Risks relating to IT access are identified, prioritised and appropriately mitigated on an ongoing basis. • Robust procedures define the access rights of individuals. • Appropriate processes are in place for new starters and leavers.
Requested additions to scope:	(if required then please provide brief detail)
Exclusions from scope:	

Planned Start Date:	18/09/2023	**Exit Meeting Date:**	21/09/2023	**Exit Meeting to be held with:**	Head of ICT

SELF ASSESSMENT RESPONSE

Matters over the previous 12 months relating to activity to be reviewed	**Y/N (if Y then please provide brief details separately)**
Has there been any reduction in the effectiveness of the internal controls due to staff absences through sickness and/or vacancies etc?	Y
Have there been any breakdowns in the internal controls resulting in disciplinary action or similar?	N
Have there been any significant changes to the process?	Y
Are there any particular matters/periods of time you would like the review to consider?	N