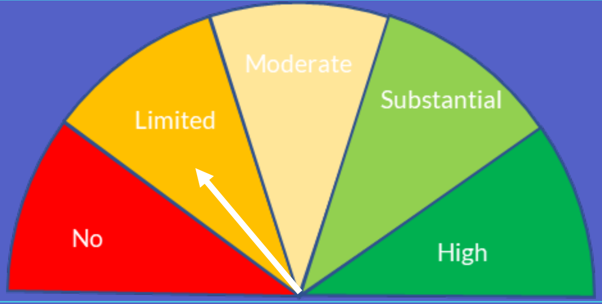
Critical Application Review – IDOX Assignment Report 2024/25 (Final)

Pendle Borough Council

902PBC_2425_903

Overall Assurance Opinion



There is a compromised system of internal control as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.

Contents

MIAA would like to thank all staff for their co-operation and assistance in completing this review.

This report has been prepared as commissioned by the organisation and is for your sole use. If you have any queries regarding this review, please contact the Engagement Manager. To discuss any other issues then please contact the Director.

1 Executive Summary

Overall Audit Objective: The overall objective of this review was to provide an assessment of the effectiveness of the control framework being exercised by management over the IDOX system and data flows and highlight improvements where appropriate.

Scope Limitation: The following areas were not considered within the scope of this review:

- Information governance, assurance reporting, risk management and legal compliance.
- Security arrangements including general interface, database security, network shares, antivirus, and patching.

Key Findings/Conclusion

The review identified that there is a compromised system of internal controls in respect of the IDOX system as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.

Areas for improvement identified included weak password credentials to access the IDOX system, a lack of user management across the system with accounts not being reviewed on a proactive basis to ensure that users still required the correct level of permissions and generic accounts had been created on the system including an administrator account.

There were also no monitoring activities carried out to provide assurance regarding the use of the system and to identify any inappropriate access.

The review also identified some areas of good practice including backups being stored in a 3-2-1 format (Three copies, two different types of storage and keeping one off site), the backups were also immutable. Third party access to the system had to be agreed prior to accessing the system via an access agreement. Remote access was granted via Cisco VPN with multifactor authentication (MFA) enabled.

Objectives Reviewed	RAG Rating
User Management including user access controls, roles, and responsibilities	Red
Logging and monitoring	Amber
Backup, resilience, recovery, and contingency (including testing and change control)	Green
Contracts, service level agreements (SLAs), assurance reporting and support arrangements	Red
Overall Assurance Rating	**Limited**

Recommendations		
Risk Rating	Control Design	Operating Effectiveness
Critical		
High	1	1
Medium	1	
Low		
Total	**2**	**1**

Areas of Good Practice

- Access to the IDOX system was managed through formal onboarding and offboarding procedures. For new starters, a request form specifying required equipment and system access was submitted to system administrators, who then create user credentials. Upon an employee's departure, a leavers form would be distributed to HR, IT, and the IDOX supervisor. The supervisor coordinated with system administrators to revoke access and reclassify the user as historic. Evidence of access removal was maintained via documented email requests.
- Role based access controls were in place across the IDOX system. Acccess controls were based on the user's role within the system and what staff can and cannot access. A sample test of ten users demonstrated that they had the correct access permissions for their roles.
- An acceptable usage message that covered all systems across the council network was displayed when a user first logs onto the network.
- Third party access must be agreed prior to accessing the system via an access agreement with the council, this was documented within the IDOX service desk support guidelines. Remote access was granted via Cisco VPN with MFA enabled, as evidenced, with examples.
- Admin level activity was monitored via Netwrix with daily reports sent to helpdesk and IDOX admin users. Screenshot evidenced demonstrated action, what item, where and who has completed the action.
- Backups were stored in two offsite locations (Fleet Street – disaster recovery (DR) site and the Wasabi Cloud Repository). A physical backup was held on site at the Parker Lane basement, fileservers and SQL servers were backed up to immutable storage.
- Council backup dashboard showed successful completion of backups that had previously been ran within a test environment, as well as backup schedules that were due to be ran. In addition to this, the council ran the failover plan which consisted of restoring from a virtual machine on a quarterly basis (02/03/2023 – 08/06/2025 evidenced).
- Backup policy / procedure (Issued 11/11/2024), included roles and responsibilities and guidelines for data backup and recovery planning. Backup schedule was also included within the policy / procedure; Daily (7-day retention), weekly (4 week rolling schedule), monthly (11 month rolling schedule) and yearly (7 years rolling schedule). Target recovery time onsite media (12 hours), target recovery time offsite media (24 hours).
- Documented processes were available for how to recover an entire Virtual Machine (VM) restore, restoring files to their original location and recovery of a physical server to VM.
- An annual review took place across the council to review the critical services for disaster recovery testing. A desktop exercise was completed in January with a DR test to be scheduled later in the year – avoiding the elections period.
- Quarterly assurance meetings were taking place between Liberata / IDOX and Pendle council, the assurance meetings consisted of roadmaps, current projects, updates, and digital notices.
- Updates regarding application maintenance / upgrades were provided via the IDOX portal and the IDOX account manager provided roadmap details. Larger upgrades were procured and managed via Project Delivery team.

Key Findings – Issues Identified	
High	1.1 The organisation had a total of twenty generic accounts on the system, including an administrator account with no further information provided on how they were monitored / managed. 1.2 Password credentials across the system were weak and did not align with NCSC best practice guidance. 1.3 There was a lack of user management across the system, accounts were not being reviewed on a proactive basis to ensure that access was required, nor were dormant accounts being reviewed and removed, where appropriate. 1.4 There was no evidence of an annual review taking place for the framework arrangement with Liberata, to ensure that the agreement in place is still relevant, contain reference to and confirms compliance with relevant legislation, such as, GDPR/DPA 2018 and reflects current arrangements. 1.5 There was no evidence of IDOX supplier assurance checks taking place such as a data protection impact assessment (DPIA), certifications check or a Digital Technology Assessment Criteria (DTAC).
Medium	1.6 At the time of the review there was currently no formalised process for the reviewing of audit trails and activity across the IDOX system. 1.7 No evidence of a logging and monitoring standard for the IDOX system

2 Findings and Management Action

1. User Management including user access controls, roles, and responsibilities		Risk Rating: High
Control Design/Operating Effectiveness		
Key Finding – We were advised that the IDOX system had twenty generic accounts on the system including Administrator and Audit profiles. Generic accounts have a lack of accountability with audit logs unable to determine a specific user carrying out activity under these accounts. Furthermore, Administrator accounts have a wider access level than a normal account resulting in attackers exploiting the wider range of privileges and permissions, making it easier to escalate their attacks once inside the network. There was no additional information provided regarding the requirement of these accounts, any additional security measures applied (e.g. no internet access, stronger password requirements) or the monitoring of activities carried out by the accounts. Password credentials to gain access to the IDOX system were weak with the following configuration settings in place; - Minimum length of six characters. - Made up of a combination of alphabetic and numeric characters.	**Specific Risk** – Failure to ensure controls are in place in respect of user access may lead to excessive permissions, unauthorised and inappropriate access and use of the system resulting in operational disruption, loss of confidential data and increased risk of a security breach.	**Recommendation –** 1. Review accounts on the IDOX system and look to remove any generic accounts. Where this is not possible, the account should have further security measures in place such as, MFA, additional monitoring, and stronger password credentials. 2. Review the password requirements to ensure it follows NCSC best practice. 3. Formalise a process for the review of accounts on a regular basis to validate the appropriateness of access rights across the IDOX system and identify accounts that are no longer required/in use.

A password that is six characters long and does not contain special characters may be at risk to a brute force attack to gain illicit access to the system. At the time of the review, there was no formal process in place for conducting periodic reviews of user accounts within IDOX. As a result, inactive, outdated, or inappropriate user access may continue to remain undetected, increasing the risk of unauthorised access to sensitive data or systems.		
Management Response – Agree that a review of generic administrator accounts should be undertaken and this number reduced if possible. Where these accounts are being used for a legitimate reason each account should be allocated to a responsible officer. Dispute the findings around passwords*. The standards you have referenced are appliable only to web based or publicly accessible systems. As IDOX must be accessed only from inside the Councils network there is no viable external attack vector. This would mean that any attacker would first have to breach the Council substantial security, remain undetected and then attempt to gain access to IDOX. The likelihood of this is very low as Council security meets the standards of Cyber Essential’s and we are undertaking a programme of hardware and software upgrades that will improve security further (Firewalls & VPN’s). Agree that accounts should be reviewed. Responsible Officer – Neil Watson Implementation Date – 31/12/2025		Evidence to confirm implementation – Review of dormant accounts across IDOX system, update the password to NCSC guidance, regular review of user access controls, review of domain administrator access to the IDOX system.

*Although the council advises it has robust network controls in place, strong password controls are also required for systems that are not accessible outside of the organisation or are behind firewalls, as they are still at risk from insider threats, credential sharing, malware/compromised endpoints, for example, that would leave a system and its data exposed.	

<table>
<tr><th colspan="2">2. Contracts, service level agreements (SLAs), assurance reporting and support arrangements</th><th>Risk Rating: High</th></tr>
<tr><td colspan="3">Control Design/Operating Effectiveness</td></tr>
<tr>
<td><b>Key Finding –</b>
The organisation provided evidence of a framework agreement between Liberata and Pendle Borough Council for the provision of software services and support. This agreement was signed in 2015 for an initial term of five years, with provisions allowing the customer to extend the duration in one-year increments.
However, there was no evidence of a formal annual review process to assess the continued relevance and adequacy of the agreement. Specifically, the agreement had not been reviewed to ensure alignment with current legislative requirements, such as the General Data Protection Regulation (GDPR)</td>
<td><b>Specific Risk –</b>
Without valid contracts/SLAs in place with suppliers, there is a risk that the council may incur additional costs / suffer financial loss in the event that the supplier has not provided the agreed upon service. Furthermore, the council cannot hold the third party to account or challenge service levels if this is not included within contract.</td>
<td><b>Recommendation –</b>
1. Confirm a valid contract is in place that is complaint with current legislation and council requirements.
2. Formalise an annual review process for the framework agreement, the review process should be documented and ensure;
○ Agreement is still relevant and covers the needs of both the organisation and supplier.
○ Compliance is up to date regarding relevant legislation.
○ Current arrangements in place are relevant (including roles and responsibilities).
○ Certifications check.</td>
</tr>
</table>

and the Data Protection Act 2018, nor to confirm that it accurately reflected current operational arrangements. In addition, there was no evidence of supplier assurance or due diligence activities being undertaken in relation to IDOX. This included the absence of a Data Protection Impact Assessment (DPIA), certification verification or evaluation against the Digital Technology Assessment Criteria (DTAC).		3. Complete a DPIA for the system and verify that certifications such as ISO27001, cyber essentials or other relevant certifications are in place for the third party.
Management Response – Will consult with Council and Liberata Contract managers on how IDOX SLA can be incorporated into the ongoing contract review process. IAR & ROPA presently under review and being updated. This will capture data processing undertaken in IDOX. Agree DPIA is needed. Responsible Officer – Karen Spencer Implementation Date – 31/1/2026		Evidence to confirm implementation – Annual review process of the framework agreement and completion of a DPIA.

3. **Logging and monitoring**		**Risk Rating: Medium**
Control Design/Operating Effectiveness		
Key Finding –	**Specific Risk** – Failure to log and pro-actively monitor activity could	**Recommendation** -

At the time of the review there was currently no arrangements in place for the review of user activity across the IDOX system, therefore any inappropriate access would not be identified such as the accessing information where there is no legitimate reason to do so. During the review, a logging and monitoring standard for the IDOX system was not evidenced for review, without this standard the council may lack consistency, reliability and clarity regarding logging and monitoring arrangements.	result in identification of issues being delayed or missed resulting in extended operational disruption, increased security incidents, loss of confidential data and breach of the GDPR.	1. Formalise a process for the regular review of user access logs to identify unauthorised activity, furthermore where possible create automated alerts to notify the council of any illegitimate access. 2. Formalise a logging and monitoring standard for the IDOX system including but not limited to; log management and event monitoring mechanisms.
Management Response – Before implementation we would first have to understand the capabilities of IDOX to identify and audit "unauthorised activity". All staff are assigned roles and given access according to their needs. Unauthorised activity needs to be considered in that context of people operating outside of their assigned roles or without permission to use Idox. Monitoring also needs to be proportionate to the limited risk. We would need to explore what built in tools there are to monitoring. Responsible Officer – Daniel Mccaffrey Implementation Date – 28/2/2026		Evidence to confirm implementation – Review of audit logs demonstrating user activity for the IDOX system, logging, and monitoring standard

Appendix A: Engagement Scope

Scope

The overall objective of this review was to provide an assessment of the effectiveness of the control framework being exercised by management over the IDOX system and data flows and highlight improvements where appropriate.

In overview, the review considered the following areas:

- User Management including user access controls, roles, and responsibilities.
- Logging and monitoring
- Backup, resilience, recovery, and contingency (including testing and change control)
- Contracts, service level agreements (SLAs), assurance reporting and support arrangements

Scope Limitations

Scope limitations included:

- Information governance, assurance reporting, risk management and legal compliance.
- Security arrangements including general interface, database security, network shares, antivirus, and patching.

Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system

Appendix B: Assurance Definitions and Risk Classifications

Level of Assurance	Description
High	There is a strong system of internal control which has been effectively designed to meet the system objectives, and that controls are consistently applied in all areas reviewed.
Substantial	There is a good system of internal control designed to meet the system objectives, and that controls are being applied consistently.
Moderate	There is an adequate system of internal control, however, in some areas weaknesses in design and/or inconsistent application of controls puts the achievement of some aspects of the system objectives at risk.
Limited	There is a compromised system of internal control as weaknesses in the design and/or inconsistent application of controls puts the achievement of the system objectives at risk.
No	There is an inadequate system of internal control as weaknesses in control, and/or consistent non- compliance with controls could/has resulted in failure to achieve the system objectives.

Risk Rating	Assessment Rationale
Critical	Control weakness that could have a significant impact upon, not only the system, function, or process objectives but also the achievement of the organisation’s objectives in relation to: • the efficient and effective use of resources • the safeguarding of assets • the preparation of reliable financial and operational information • compliance with laws and regulations.
High	Control weakness that has or is likely to have a significant impact upon the achievement of key system, function, or process objectives. This weakness, whilst high impact for the system, function or process does not have a significantimpact on the achievement of the overall organisation objectives.
Medium	Control weakness that: • has a low impact on the achievement of the key system, function, or process objectives; • has exposed the system, function, or process to a key risk, however the likelihood of this risk occurring is low.
Low	Control weakness that does not impact upon the achievement of key system, function, or process objectives; however, implementation of the recommendation would improve overall control.

Appendix C: Report Distribution

Name	Title
Karen Spencer	Director of Resources
Marie Mason	Corporate Client and Performance Manager
Howard Culshaw	Head of Legal and Data Protection Officer
Dean Langton	Chief Executive
Neil Watson	Assistant Director of Planning, Building Control and Regulatory Services
Phillip Spurr	Director of Place

Gemma Owens
Principal Digital Risk Consultant
Tel: 07717 720 389
Email: Gemma.Owens@miaa.nhs.uk

Conor Finegan
Technology Risk Assurance Auditor
Tel: 07825 100 276
Email: Conor.Finegan@miaa.nhs.uk

Paula Fagan
Assistant Director – Digital
Tel: 07825 592 866
Email: Paula.Fagan@miaa.nhs.uk

Limitations

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

Global Internal Audit Standards (UK public sector)

Our work was completed in accordance with Global Internal Audit Standards (UK public sector).