INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Cloud Applications
TO:	System Owners	**DATE:**	25 October 2019
C.C.	Deputy Chief Executive (AJ) Chief Executive Head of Finance Democratic Services Manager Arts Manager Portfolio Holder – Cllr Day		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2019/20 an audit review of cloud applications was completed in September 2019. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 This audit was undertaken to ensure that adequate controls are in place to protect the security, integrity and availability of data stored on Council cloud-based applications.

3 Scope and Objectives of the Audit

3.1 The audit was designed to assess and provide assurance on the following key areas:

- Information security guidelines on Cloud applications
- Access control including two factor authentication
- Proxy server protection to prevent access to insecure or unauthorised cloud applications
- External security testing
- Resilience and Disaster Recovery protection
- 3rd party Contracts including confidentiality and GDPR agreements.

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

4 **Findings**

4.1 **Recommendations from Previous Report**

4.1.1 This section is not applicable as this the first audit of this area.

4.2 **Information security guidelines**

4.2.1 Key ICT policies and procedures relevant to the management and security of cloud-based applications were identified and obtained during the course of the audit. These were used in the process of reviewing the adequacy and completeness of the controls in place around cloud applications.

4.2.2 The policies identified as being of particular relevance in this review are the; 'Information Security and Conduct Policy', 'Privacy Impact Assessment Toolkit', and the 'Software Policy'.

4.2.3 Of the policies and procedures obtained and reviewed during the audit it was noted that the 'Privacy Impact Assessment Toolkit' document requires review and updating to reflect changes in the processes and procedures since the last update and to reference GDPR.

Risk

The privacy impact assessment process may be inconsistently performed.

Recommendation

The 'Privacy Impact Assessment Toolkit' document should be reviewed and updated.

4.2.4 It was also noted that the current version of the 'Software Policy' does not mention the privacy impact assessment process or reference the 'Privacy Impact Assessment Toolkit' document.

Risk

Privacy impact assessments may not be performed leading potential breaches of DPA and/or GDPR requirements.

Recommendation

The 'Software Policy' should be updated to reference the 'Privacy Impact Assessment Toolkit' process.

4.3 **Access control including two factor authentication**

4.3.1 Two cloud-based applications were selected in conjunction with management to be the basis for review as part of this audit. These were the ArtifaxEvent and Get Scheduled applications.

4.3.2 An understanding of the system management and access control arrangements in place for the applications tested was obtained through discussion with ICT and system owners and review of available process documentation.

4.3.3 User set up, change and removal processes were walked through and key application security controls including authentication controls and password settings were obtained and reviewed for each of the systems tested. This highlighted the issues detailed below.

4.3.4 It is good security practice to ensure complex passwords are in use and enforced by strong password security controls. A review of 'Get Scheduled' password parameters identified the system does not currently enforce strong password complexity requirements.

Risk

There may be unauthorised access to application data due to the use of weak passwords.

Recommendation

Management should liaise with the supplier to increase Get Scheduled password complexity requirements.

4.3.5 It was noted that the ArtifaxEvent application has the facility to implement two factor authentication but that this was not currently in use. It is recommended that management consider implementing this in order to provide improved security.

Risk

There may be unauthorised access to application data due to the use of weak passwords/ password sharing.

Recommendation

Management should investigate options around implementing two-factor authentication to the ArtifaxEvent application.

4.4 External security testing

4.4.1 An annual exercise of external penetration testing of the Council's infrastructure is undertaken as part of the annual IT Health Check (ITHC) exercise required as part of the PSN accreditation process. This is used to ensure the Council network is adequately protected against known vulnerabilities.

4.4.2 Additional ad hoc vulnerability scanning and penetration testing exercises are performed in conjunction with third party consultants on a risk basis, where deemed necessary throughout the year.

4.4.3 The two applications focused on as part of this audit are cloud-based services hosted by external suppliers, meaning the Council is reliant on the third party to secure the data appropriately.

4.4.4 A privacy impact assessment process is in place for use when implementing or making changes to systems, enabling management to gain some assurance around the security of data being held and processed. It was found during the work that this exercise had been completed for the Get Scheduled application but not ArtifaxEvent.

4.4.5 Although the risk is mitigated to some extent by the fact that the Council moved to a cloud-hosted service provided by the existing supplier that provided the previous version of the system, it is recommended that the privacy impact assessment be completed to ensure all privacy and security issues have been considered and documented.

Risk

Personal data may be held insecurely and/or breach DPA requirements.

Recommendation

The privacy impact assessment process should be completed retrospectively for the ArtifaxEvent system.

4.5 **Resilience and Disaster Recovery protection**

4.5.1 It was confirmed during testing that for both ArtifaxEvent and Get Scheduled backups of data and recovery arrangements are included as part of the service provided by the supplier. No recent outages or significant downtime was reported by management for either application.

4.6 **3rd party Contracts**

4.6.1 The contract and terms and conditions in place in relation to the Get Scheduled application were obtained and reviewed as part of the audit. It was found to have undergone review by the Council's procurement and information governance teams and to include the required references to GDPR obligations around data security.

4.6.2 It was not possible to obtain the ArtifaxEvent contract in the timescale required for this review. It is recommended that the privacy impact assessment recommended above (4.4.5) includes a review of the contract to ensure it meets Council requirements.

5 **Conclusions**

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did, however, identify four Medium rated and one Low rated issues which, if addressed, would improve the overall control environment.

Overall, the findings are considered to give MODERATE assurance around the management of cloud applications.

5.1 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above, are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Cloud Applications – October 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	System Owner Response	Target Date
4.2.3	The ‘Privacy Impact Assessment Toolkit’ document should be reviewed and updated.	The privacy impact assessment process may be inconsistently performed.	Medium	Information Governance Manager (Shafim Kauser)	The review of the toolkit is currently under way, along with the rest of the Information Governance Framework, and this will be completed by 23 December 2019.	23 December 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	System Owner Response	Target Date
4.2.4	The ‘Software Policy’ should be updated to reference the ‘Privacy Impact Assessment Toolkit’ process.	Privacy impact assessments may not be performed leading to potential breaches of DPA and/or GDPR requirements.	Low	ICT Services Manager (Ty Walter)	Accepted: The Software Policy has been updated to reflect the PIA Toolkit requirements (03 Oct 2019), and this version is now available via the ICT Policy pages on the Intranet.	Not applicable.

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	System Owner Response	Target Date
4.3.4	Management should liaise with the supplier to increase Get Scheduled password complexity requirements.	There may be unauthorised access to application data due to the use of weak passwords.	Medium	Get Scheduled System Owner (Jessica Craddock)	I had spoken with the system owner and system developer (Tom Douglas & Wojciech Dragan) to implement the complexity requirements. Passwords for each user now requires a minimum of 8 characters including 1 special character, 1 uppercase and 1 number. This was actioned by all users w/c 23.09.19.	Not applicable – recommendation actioned.

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	System Owner Response	Target Date
4.3.5	Management should investigate options around implementing two factor authentication to the ArtifaxEvent application.	There may be unauthorised access to application data due to the use of weak passwords / password sharing.	Medium	ArtifaxEvent System Owner (Laura Wyatt)	We have tested the two-factor authentication provided by the ArtifaxEvent system. As the system heavily relies on mobile phone signage and the phone reception at the Royal Spa Centre being so poor we are unable to switch this on. It would potentially mean locking our users out of the system when they required necessary information for events.	Not applicable – recommendation not accepted.
4.4.5	The privacy impact assessment process should be completed retrospectively for the ArtifaxEvent system.	Personal data may be held insecurely and/or breach DPA requirements.	Medium	ArtifaxEvent System Owner (Laura Wyatt)	To be arranged and completed.	31 December 2019

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.