ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	14 February 2019
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC1912 – Data Security in a Cloud Based Environment
REPORT NUMBER	IA/AC1912
DIRECTOR	N/A
REPORT AUTHOR	David Hughes
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on Data Security in a Cloud Based Environment.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. BACKGROUND / MAIN ISSUES

3.1 Internal Audit has completed the attached report which relates to an audit of Data Security in a Cloud Based Environment.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are as detailed in the attached appendix.

7. OUTCOMES

7.1 There are no direct impacts, as a result of this report, in relation to the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place, or Enabling Technology, or on the Design Principles of the Target Operating Model.

7.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

8. IMPACT ASSESSMENTS

Assessment	Outcome
Equality & Human Rights Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required
Duty of Due Regard / Fairer Scotland Duty	Not applicable

9. APPENDICES

9.1 Internal Audit report AC1912 – Data Security in a Cloud Based Environment.

10. REPORT AUTHOR DETAILS

David Hughes, Chief Internal Auditor
David.Hughes@aberdeenshire.gov.uk
(01467) 537861

Internal Audit Report

Digital and Technology

Data Security in a Cloud Based Environment

Issued to:
Andy McDonald, Director of Customer Services
Andrew Howe, Chief Officer – Digital and Technology
Norman Hogg, Security Architect
Caroline Anderson, Information and Data Manager
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
External Audit

Date of Issue: May 2019 **Report No. AC1912**

EXECUTIVE SUMMARY

The objective of this audit was to provide assurance over the Council's arrangements to ensure data security where business is transacted through the Cloud. *The Council uses both the private cloud through their data centre service provider and the public cloud through externally hosted applications.*

Whilst a number of controls were in place in relation to: policies and procedures (with the exception of minor updates); data protection training; governance arrangements; procurement arrangements for systems subject to tender or procured from a government framework agreement; and back up and system patch management arrangements based at the Council data centre provider; recommendations have been made to improve the data security monitoring arrangements.

An ICT System Risk Assessment is required to be completed, to ensure adequate technical and physical measures are in place, to secure and protect information assets. New systems must be authorised by Digital and Technology (D&T) before use and in the case of systems with a value greater than £50,000, invitation to tender security question responses cover the requirements of an ICT System Risk Assessment, including disaster recovery; data backup arrangements; and data security audit arrangements. Where systems are not procured via government frameworks or a tender, whilst system approval by D&T is required, the ICT System Risk Assessment undertaken by D&T before system approval was not documented. As part of the on-going process to revise the Information Asset Register, D&T and Information Governance have agreed to include all Council systems, describing the nature of the data held, and the adequacy of technical and physical measures to secure that data.

Whilst due diligence is undertaken at the procurement stage for cloud based systems in relation to system backup and disaster recovery, it was noted that a disaster recovery plan was not available for one public cloud based system reviewed. In addition, arrangements for gaining on-going assurance over data back-up success and disaster recovery testing for public based cloud suppliers has not been formalised and with the exception of the Planning Consultation System, there was no evidence of these areas being monitored. This is particularly relevant for business critical systems moved into the public cloud. The Cluster concerned has agreed to obtain the relevant business continuity plan and D&T will seek assurances from system owners in relation to back-up and disaster recovery.

It is a requirement of GDPR to ensure a process is in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data being processed. D&T has arranged for an independent assessment of cyber security arrangements (IT health checks / penetration test) in relation to the Council's Customer Experience Platform. Penetration testing has not been arranged for other cloud-based suppliers holding Council personal data, however the intention is to schedule testing for Office 365 and the new Human Capital Management system. Certain public cloud based suppliers, such as Microsoft, publish regular security audits, however D&T do not presently monitor these reports. Internal Audit recommended that IT health check reports and security audits should be arranged / monitored by D&T as the Cluster is best qualified to interpret the results. However, D&T believe any ongoing assurance for data security should be managed by the relevant Cluster as part of account meetings with system providers and through contract management.

Only two business critical systems maintained by the data centre provider had been subject to disaster recovery testing in 2018. The Cluster advised that system

upgrades and server changes are being carried out before the remaining systems can be subject to disaster recovery testing and have agreed to schedule testing once these upgrades and server changes are complete.

In order to assess the risk of transferring data to the cloud, data protection impact assessments (DPIAs) should be completed for Information Assets that contain personal data before doing so. The DPIA for one cloud-based system did not identify where personal data is stored as required. Four other cloud-based systems did not have DPIAs in place. The Clusters concerned have agreed to update / complete DPIAs as required. In addition, the public cloud-based Housing Advice and Support System was replaced in March 2019 however confirmation has not been obtained from the previous provider that all Council data has been destroyed. The Service has agreed to obtain this.

Contractual arrangements with a sample of public cloud-based hosted systems and the Council's data centre provider were reviewed, to ensure that the contracts in place and the invitation to tender responses and assessments where required, enabled compliance with the GDPR data security requirements, the processing and storage of personal data was specified, and that the systems were approved for use by D&T. This was found to be the case with the exception of the Early Years Admission and Enrolment system, where a copy of the contract was unavailable. The Cluster has agreed to obtain a contract detailing how the Council's data is processed and stored.

1. INTRODUCTION

1.1 The objective of this audit was to provide assurance over the Council's arrangements to ensure data security where business is transacted through the Cloud.

1.2 In April 2014 the Scottish Government published the Data Hosting and Data Centre Strategy for the Scottish Public Sector. The strategy's vision was for Scotland's public sector data hosting to be cost-effective, carbon neutral and make appropriate use of cloud technology. The Scottish Government's March 2015 Scottish Public Sector Cloud Guidance includes the following potential benefits: access to shared computing resources from any location; freedom from capital expenditure on back-end computing equipment and software; the ability to source computing services quickly and cheaper than traditional models; and the ability to pay for such services on some form of metered or per-use basis. The Guidance goes on to state that organisations must consider how they can adopt cloud computing to deliver the efficiency and flexibility it can offer.

1.3 The term "cloud technology" indicates services are being delivered over the internet rather than from an organisation's own on-site data centre. The Scottish Government adopts the "cloud computing" definition provided by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access, to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

1.4 The Scottish Public Sector Cloud Guidance details security considerations when using the cloud, including confidentiality (organisations specifying where data is stored to avoid loss / corruption of data); integrity (data sufficiently portable to avoid vendor "lock-in"); availability (reliable access to data e.g. good internet connectivity); and having appropriate contractual arrangements.

1.5 There are four deployment models for the Cloud:

- Public – where resources are available to any customer;
- Private – where resources are exclusively used and controlled by one customer;
- Community – where resources are shared between a group of similar customers with shared objectives; and
- Hybrid – a composite of two or more of the other cloud models.

The Council uses both the private cloud through their data centre service provider and the public cloud through externally hosted applications.

1.6 The factual accuracy of this report and action to be taken regarding the recommendations made have been agreed with Andrew Howe, Chief Officer – Digital and Technology, Norman Hogg, Security Architect, Steven Robertson, Infrastructure Architect, and Caroline Anderson, Information and Data Manager.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Policies and Procedures

2.1.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance that correct and consistent instructions are available to staff, important in the event of an experienced employee being absent or leaving. They have increased importance where new systems or procedures are being introduced.

2.1.2 The ICT Acceptable Use Policy defines employee responsibilities when using Council ICT equipment, networks and systems. The policy is comprehensive and includes appropriate user behaviour (use of passwords, use of email, locking ICT equipment etc), monitoring arrangements in place to ensure compliance with the policy, and reporting requirements in relation to breaches and incidents. In addition, the policy requires employees to only make use of ICT equipment, systems and networks that have been authorised for use by Digital & Technology (D&T). This is considered further in section 2.4.

2.1.3 Other policies are in place relating to data security, including: the Corporate Information Policy, which details governance arrangements in relation to the Council's information and data; the Corporate Protective Monitoring Policy, which details the means of collecting, analysing and reporting on threats to the Council's data; and the ICT Access Control Policy, which details the expected controls and employee behaviour, to avoid unauthorised access to Council data. These policies and the ICT Acceptable Use Policy are comprehensive.

2.1.4 It was noted that the ICT Acceptable Use Policy and the Protective Monitoring Policy had not been reviewed as scheduled and there were some minor amendments required to the policies in relation to references to: historic data protection legislation (in addition to correctly referring to GDPR); historic risk registers; and the Finance, Policy and Resources Committee as the Committee with approval authority for the ICT Acceptable Use Policy. A recommendation is included for tracking purposes.

Recommendation
The ICT Acceptable Use Policy and Protective Monitoring Policy, should be reviewed, updated and approved as appropriate.

Service Response / Action
The minor changes to these documents are in plan with an aim to review at the next Information Governance Group meeting.

Implementation Date	Responsible Officer	Grading
Implemented	Security Architect	Important within audited area

2.1.5 A number of procedures are also in place to help ensure Council data remains secure, including: the Managing Information Handbook; the Information Security Incident Reporting procedure; and the Information Asset Owner Handbook. These procedures make Council employee responsibilities clear in relation to data security, including where data is shared with cloud-based systems.

2.2 Training

2.2.1 The mandatory Information Governance training, which covers data protection requirements under the General Data Protection Regulation, is required to be completed

by all employees. Completion statistics are reported quarterly to the Information Governance Group and monthly to Corporate Management Team (CMT), as part of risk Corp-005 Information Governance, included in the Corporate Risk Register. Training completion of 44% was reported in the Information Governance Management Annual Report to the Audit, Risk and Scrutiny Committee on 25 September 2018. More recently, training completion was 88%, as reported to CMT on 28 March 2019.

2.2.2 Information Governance advised that exception reports are sent to Chief Officers on a monthly basis, with details of employees yet to complete the Information Governance training, to help ensure that training is completed as required. A sample of Chief Officers was selected and all had received these reports as expected in January 2019.

2.3 Risk

2.3.1 The Corporate Risk Register is reported to CMT on a monthly basis. This includes risk Corp-006 relating to Cyber Security, defined as "Cyber Security threats must be mitigated to protect the Council, its essential functions and customer data". A potential cause highlighted is a lack of appreciation of the threats of extension into the Cloud. The potential impact includes service disruption, unlawful disclosure of sensitive information, individuals placed at risk of harm, prosecution, reputational damage, and financial penalties. The Service has assessed risk Corp-006 Cyber Security as very serious with a low likelihood based on the controls in place, which are detailed in the Corporate Risk Register, along with an assessment of how effective the controls are.

2.3.2 The Customer risk register by Cluster (Cluster Risk Register), last reported to the Operational Delivery Committee on 6 November 2018, also includes the risk of service disruption potentially caused by moving to external cloud-based services. It has since been updated and the version as at 11 April 2019 states "as Services move out to the Cloud, the risks to data increase, as the security boundary is expanded and we have reduced visibility into what happens." Required controls are stated to include a sound Identity Access Management System (IDAM) combined with role-based access and identification, and investigation of anomalous behaviour.

2.3.3 The Cluster Risk Register's control actions state that Identity Management is controlled by a number of systems and that anomalous behaviour techniques are in operation, through the use of the IDAM solution, Office 365, and changes to the Council's private data centre provision, as these are rolled out. Examples of anomalous behaviour analytics include: requiring a user to provide further evidence of their identity, should they change the device they use to log in; or preventing access if a user logs in more than once, from geographically distant areas, in quick succession.

2.3.4 The IDAM solution will link into Office 365, the Active Directory used to identify users when logging into their devices, and the Human Capital Management System. It will be used to manage account creation, changes and deletions, via the Human Capital Management system. When the Human Capital Management system is updated with a starter, leaver or mover, the IDAM solution will identify this and automatically create, remove or amend the user's network account, email account, and rights and privileges as appropriate. The IDAM solution will determine access to corporate drives, Office 365 and any other platform that uses the Active Directory for access based on the user's role.

2.3.5 The Cluster Risk Register reported that progress with implementing the IDAM solution and behavioural analytics was 20% complete with a target completion date of 31 July 2019. The Service has advised that this is now 40% complete as a result of some Office 365 monitoring, alerting and behavioural analysis being implemented and the IDAM solution now being in the testing phase. The target completion date is still 31 July 2019, although the solution will then have to be developed over time to increase and confirm security.

2.3.6 According to the Corporate Information Policy, the Senior Information Risk Owner (SIRO) is accountable to the Chief Executive for the management of the information risks across the Council. To achieve this the SIRO must ensure that the Council's Information Asset Owners are carrying out their roles effectively and consistently implementing information risk processes. Information Asset Owners are required to provide assurance to the SIRO on the use, management and governance of their information assets, to enable the SIRO to report to the Chief Executive. A checklist is available in the Information Asset Owner Handbook which details expected actions by the Information Asset Owner in order to provide this assurance, including:

- the Information Asset Register is up to date;
- Privacy Impact Assessments have been completed where required in relation to data protection;
- contractual arrangements are in place with third parties involved in processing, hosting or supporting the Information Asset;
- it is known who has access to information and why;
- appropriate disaster recovery and business continuity arrangements are in place;
- the Information Asset Owner is satisfied with the technical and physical measures in place to secure and protect the Information Asset; and
- risks in relation to Information Assets are actively managed with risk registers updated as appropriate.

2.3.7 Information Governance has advised that confirmation of technical and physical measures being in place, to secure and protect an Information Asset, is no longer going to be an Information Asset Owner's responsibility, as part of the Information Asset Assurance statement, as Digital and Technology must assess the system before this can be determined.

2.3.8 The Corporate Information Policy defines Information Asset Owners as senior business managers responsible and accountable for the specific, defined information assets within their remit, in accordance with the Council's Information Asset Owner Handbook (the Handbook). The Handbook defines an Information Asset as an identifiable collection of data stored in any manner, at any location (i.e. including private and public cloud), which is recognised as having value to the Council for the purposes of performing its business functions and activities. All collections of information containing personal information must be managed as Information Assets.

2.3.9 Information Asset Owners are required by the Handbook to register and keep up to date entries relating to their information assets in the Council's Information Asset Register. In a sample of three public cloud-based systems (Microsoft Office 365, the Customer Experience Platform, and the Planning Consultation System) used to store Council data, two were present on the register, whilst the Microsoft Office 365 OneDrive was not, despite approximately 2,300 employees having access to it.

2.3.10 Microsoft OneDrive is the new employee personal drive which has been rolled out and replaced the B drive on 15 March 2019. The information stored on Office 365, including the OneDrive, the value of the information stored to the Council, the legal basis for it being stored, and the location of the data being saved are not recorded on the Information Asset Register as required. The guidance regarding the transfer of data from the B Drive to OneDrive states that personal drives have historically been used to store personal work-related documents, including personal review and development documents and contracts of employment. This is in line with the Managing Information Handbook which states personal drives should be used for work-related personal information (not Council information) which cannot be stored on the shared drive for confidentiality reasons. The

guidance only recommends documents which are not work related be removed meaning personal data will be recorded on OneDrive.

2.3.11 Whilst it was noted that Office 365 was absent from the Information Asset Register despite holding personal data, it was also noted the performance information system, recorded on the register as containing personal sensitive data in relation to pupil case files, did not contain this data.

2.3.12 Management has stated that the Information Asset Register is currently under review. Information Governance and D&T are collaborating to develop a database which is more focused on the flow of data. This will include all relevant details for each Information Asset, including the means by which data is captured; the relevant privacy notice to notify the public of data being captured; the system used to store and process the data; adequacy of technical and physical measures to secure Information Assets; and the reasons, means and legal basis for processing.

2.3.13 Information Governance has contacted Information Asset Owners of Information Assets deemed to be high risk by Information Governance, in relation to the flow of data, to confirm the following are in place: local procedures; retention and disposal arrangements; Information Sharing protocols (where applicable); a privacy notice; and any relevant contracts are included on the contracts register. The intention is to collaborate with D&T to capture relevant details in relation to systems holding Information Assets.

2.3.14 The Handbook recommends that an ICT System Risk Assessment be used by Information Asset Owners to ensure they are satisfied that the technical and physical measures in place to secure and protect their information assets are adequate. The Information Asset Register will capture the outcome of these assessments prior to systems being authorised for use by D&T, as required by the ICT Acceptable Use Policy. A recommendation is included for tracking purposes.

Recommendation
Information Governance should liaise with D&T to establish a revised Information Asset Register that reflects all Council systems, describing the nature of the data held in Council systems and the adequacy of technical and physical measures to secure that data.

Service Response / Action
Agreed. The Service will look to document achievement of "baseline" technical and physical measures in accordance with the Scottish Government Cyber Resilience Framework to be released later this year.

Implementation Date	Responsible Officer	Grading
December 2019	Information and Data Manager Security Architect	Significant within audited area

2.3.15 The Handbook requires a privacy impact assessment to be completed where information assets contain personal data and there is to be a change in the way the information is collected, stored, used, managed or processed, such as transferring Council personal data to a third party. Privacy impact assessments / Data Protection Impact Assessments were requested for a sample of cloud-based systems (Microsoft Office 365; Customer Experience Platform, Human Capital Management System, Planning Consultation System, Housing Advice and Support System, Music Tuition Database, and the Early Years Admission and Enrolment System). Three assessments were available for review, with two having been completed as required, one assessment was partially completed, and four assessments were unavailable for review.

2.3.16 The Data Protection Impact Assessment for Microsoft Office 365 did not identify where personal data is stored and protected as required. The Mini-Competition Invitation for the Council's Microsoft Enterprise Agreement, under which Office 365 was procured, states that the Council note that any software delivered under the contract will be covered by the standard Microsoft Terms and Conditions. The Microsoft Online Services Terms states that Office 365 customer data is located in the UK at rest, however the data may be transferred to the United States or any other country in which Microsoft or its Sub Processors operate, to provide the Online services. Whilst Microsoft states that safeguards are in place in compliance with GDPR, the fact that data is transferred in this way has not been assessed in the Data Protection Impact Assessment, to determine if it is suitable for the Council.

2.3.17 Google Apps for Education is a public cloud-based service, which is used by the Council to store personal information relating to Aberdeen City pupils and staff. One of its uses is to store the Council's Music Tuition Pupil Spreadsheet, which contains: pupil names; schools; year; home address; and parent email addresses. Google may store and process Customer Data in the United States and any country in which Google or any of its Sub Processors maintains facilities, as confirmed by Governance in an initial privacy impact need assessment. The assessment concluded Google's terms and conditions were acceptable from a legal perspective. The initial assessment was also completed by the Cluster who concluded a privacy impact assessment was not required. The Cluster now intend to review the risks by completing a full data protection impact assessment.

2.3.18 The Housing Advice and Support System was replaced in March 2019 from a public cloud-based system to a secure file sharing system, used to share data using the Council's private cloud data centre. Homeless client names and details of the hours of support provided, are uploaded to the Council's data centre, by external providers of that support, using the secure file sharing software, in order for the Council to access that data. A Privacy Impact Assessment was not completed prior to transferring the data from the previous system. It was also noted that confirmation is yet to be obtained from the previous hosted system provider that all Council data has been destroyed.

2.3.19 A data protection impact assessment has not been completed for the Early Years Admission and Enrolment System since the use of the system pre-dates the requirement for a DPIA. Invitation to tender documentation was unavailable therefore it was not possible to determine if data security arrangements had been adequately considered as part of the procurement process.

2.3.20 A data protection impact assessment was unavailable in relation to the Planning Consultation system. It is therefore not possible to determine if data protection has been adequately considered in relation to the use of the system.

Recommendation

a) Data Protection Impact Assessments should be completed where personal data is to be managed differently.

b) Confirmation should be obtained from former cloud-based system providers that Council data has been destroyed once transferred.

c) Integrated Children's and Family Services should arrange for a DPIA and ICT System Risk Assessment to be completed for the Early Years Admission and Enrolment System.

Service Response / Action

Agreed

Implementation Date	Responsible Officer	Grading
July 2019	a) Data Centre Transition Manager / Quality Improvement Officer / Development Team Leader / Chief Officer Strategic Place Planning b) Development Officer Contracts c) Early Years Manager	Significant within audited area

2.3.21 As described at paragraph 2.3.10 Council data has been transferred to Microsoft as part of the rollout of OneDrive, which is to replace the personal "B" drives. A pilot is also underway within Digital and Technology to rollout Microsoft Office 365 Sharepoint as a replacement for the existing shared "0" drive. D&T expect this pilot to be completed by 31 May 2019, after which Sharepoint will be rolled out to all Clusters. Data Stewards at a Service Area level have been asked to review the folders within their remit, and classify them as to be moved into Sharepoint, deleted or archived. The Service Area that the folders relate to must also be identified as well as the Business classification and retention period. In all cases the retention period has a link to the Information and Communication Technology page of the Council's Retention and Disposal Schedule.

2.3.22 Microsoft Office 365 has the functionality to classify files according to confidentiality, using sensitivity labels, resulting in restriction of access to data to specified users as required, and for retention periods to be defined after which files are automatically deleted, using retention labels. Files are not being classified using this functionality of Office 365, as part of the rollout of Sharepoint and OneDrive, due to the scale of the work required to complete the initial rollout. The Cluster will give consideration to classifying files in this way following the rollout of Sharepoint and OneDrive.

2.4 Procurement

2.4.1 Article 32 of GDPR requires the data controller and processor to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (considered further in section 2.7);
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (considered further in section 2.5); and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (considered further in section 2.6).

2.4.2 GDPR Article 28(3) and section 59(5) of the DPA 2018 require that where a data controller such as the Council uses a third party to process personal data, the processing should be governed by a contract, binding the processor to the controller and setting out the subject

matter and duration of processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller.

2.4.3 As stated in paragraph 2.1.2, the ICT Acceptable Use Policy requires employees to only make use of ICT equipment, systems and networks that have been authorised for use by Digital & Technology (D&T).

2.4.4 Contractual arrangements with a sample of public cloud-based hosted systems and the Council's data centre provider were reviewed, to ensure that the contracts in place and the invitation to tender responses and assessments where required, enabled compliance with the GDPR data security requirements detailed in paragraph 2.4.1, the processing and storage of personal data was specified, and that the systems were approved for use by D&T. This was found to be the case with the exception of the Early Years Admission and Enrolment system, where a copy of the contract, detailing how Council data was being processed and stored, was unavailable.

Recommendation A copy of the contract between the Early Years Admission and Enrolment system and the Council, detailing how Council data is processed and stored, should be obtained.		
Service Response / Action Agreed.		
Implementation Date July 2019	**Responsible Officer** Early Years Manager	**Grading** Significant within audited area

2.4.5 The suppliers were also reviewed to ensure they had internationally recognised certification, in relation to managing data security risks. All cloud-based providers reviewed had advised they had at least current ISO27001:2013 certification, indicating they had an adequate information security management system.

2.5 Back Up and Disaster Recovery

2.5.1 Article 32 of GDPR requires the data controller and processor to implement appropriate technical and organisational measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

2.5.2 Private cloud business critical systems are backed up in full on a weekly basis and incrementally on a daily basis by the Council's Data Centre provider, with 30 days of back up files held locally in Aberdeen and a 90-day offsite retention held in the disaster recovery datacentre in Dundee.

2.5.3 ICT receives daily emails detailing the status of the back-ups for the systems managed by the Council's data centre provider and any exceptions in relation to failed back up attempts.

2.5.4 A schedule of systems to be tested for Disaster Recovery, in the 4-year period to 2020, has been set up, with testing dates included where known. It was noted that a number of systems had not been scheduled for testing in 2018 and 2019. The Cluster advised testing is never scheduled beyond the following year as testing dates are usually subject to change. The case management system for Social Work and the Child Protection Register had been subject to disaster recovery testing in 2018. The Cluster advised that system upgrades and server changes are being carried out before the remaining systems can be subject to disaster recovery testing.

2.5.5 D&T seek to gain assurance over technical and physical measures in place to protect information assets, for procurements of greater than £50,000, via Invitation to Tender (ITT) data security question responses and supporting documentation provided by those suppliers. The ITT data security questions include a requirement for disaster recovery to be built into the system and for the system to have off-site backups consisting of transaction logs, incremental backups and full backups. Where the Crown Commercial Service G-Cloud framework agreement has been used to procure public cloud based services, it is a requirement of that framework that the supplier have a clear disaster recovery plan in place. In addition, employees are required to seek authorisation from D&T before making use of new ICT systems and networks.

2.5.6 Whilst due diligence is undertaken at the procurement stage for these systems, arrangements for gaining on-going assurance after the procurement stage, over data back-up success and disaster recovery testing for public based cloud suppliers, has not been formalised and with the exception of the Planning Consultation System, where backup success was reported as part of the monthly Managed Services Service Review report to the Cluster, there was no evidence of disaster recovery testing and back-up success being monitored for public cloud based systems. This is particularly relevant for business critical systems moved into the public cloud. Reports of backup restore points were unavailable for the Customer Experience Platform, Music Tuition system, and Early Years Admission and Enrolment System.

2.5.7 Supplier business continuity plans were in place, for the Human Capital Management system, Office 365, the Music Tuition system, the Planning Consultation System and the Customer Experience Platform. However, a plan was unavailable for the Early Years Admission and Enrolment System.

Recommendation

a) Disaster recovery testing should be scheduled with the Council's data centre provider for business-critical systems.

b) Success of back-ups and disaster recovery testing should be monitored where data is held with public cloud-based system providers.

c) A supplier business continuity plans should be obtained for the Early Years Admission and Enrolment System.

Service Response / Action

a) Agreed. The Child Protection Register and Carefirst have been provisionally booked for testing in November 2019.

b) System owners will be asked to contact their vendors to gain ongoing assurance over backup success and disaster recovery testing for public cloud based systems.

c) Agreed.

Implementation Date	Responsible Officer	Grading
a) November 2019	a) Incident and Problem Co-ordinator	Significant within audited area
b) Implemented	b) Incident and Problem Co-ordinator	
c) July 2019	c) Early Years Manager	

2.6 Data Security Monitoring

2.6.1 As stated in paragraph 2.4.1, it is a requirement of GDPR to ensure a process is in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data being processed.

2.6.2 IT Health Checks provide an independent assessment of an organisation's cyber security arrangements. ITHC reports can provide assurance that cloud-based service provider systems are protected from unauthorised access or change. D&T arranged for the Council's IT Health Check provider to carry out a penetration test of the hosted Customer Experience Platform. The Information Asset Owner for the system has indicated consideration is being given to commencing regular penetration testing of the platform and that this is being put out to tender as part of a wider IT Health Check and Cyber Essentials Plus service.

2.6.3 Penetration testing is yet to be scheduled for the new Human Capital Management System, which has been procured, but is yet to go live. The supplier has advised that historic penetration testing is not available and that the Council, like its other customers, would have to make arrangements for penetration testing to be carried out by a third party of its choice. This is due to the fact that each customer has a bespoke data security environment depending on account security settings.

2.6.4 D&T confirmed that IT health checks, or penetration testing, has not been monitored for other cloud-based suppliers holding Council personal data. Audits of the data processing undertaken on Council data by the cloud provider of the Music Tuition system are allowed under the standard contractual terms, however such an audit has not taken place. D&T intends to schedule penetration testing for Office 365 and the Council's Human Capital Management system.

Recommendation
D&T should arrange and monitor IT health check reports / security audits for third party suppliers managing Council personal data in the cloud as required.

Service Response / Action
D&T arrange Council initiated external checks on systems as deemed appropriate by the service. Suppliers themselves are responsible for their own checks and where necessary are stated as requirements when going out for procurement. D&T believe any ongoing assurance around this should be sought by the services as part of their regular or annual account meetings and contract management. D&T have no direct relationship with the providers.

Internal Audit Position
As per 2.3.7 Information Asset Owners are no longer considered to be responsible for confirming the adequacy of technical and physical measures to secure and protect Information Assets, D&T are best qualified to determine if systems have adequate data security measures in place during the life of contracts with public cloud-based suppliers. This is particularly relevant for business critical systems moved into the public cloud.

Implementation Date	Responsible Officer	Grading
N/A	N/A	Significant within audited area

2.6.5 Every system maintained at the Council's data centre provider has patches applied once every four weeks on a rolling 4-week cycle. Patches are required to resolve system security vulnerabilities. The success of patches is checked weekly. This was primarily a manual process and untracked. The Security Architect has since developed a report

which identifies whether patches, for all relevant systems, have been successfully applied and has advised that this will be reported to ICT Management on a monthly basis.

2.6.6 The IT Security Architect and Infrastructure Architect are members of the Local Authorities Information Security Group, the Cyber Security Information Sharing Partnership, and subscribe to a number of live feeds, providing updates every 15 minutes, that will detail any new cyber threats requiring action. Should data security incidents be reported, that affect the cloud providers used by the Council, the Security Team can take appropriate action.

2.7 System Performance

2.7.1 As stated in paragraph 2.4.1, it is a requirement of GDPR for the Council to ensure arrangements are in place for the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

2.7.2 The performance availability of Council servers and networks used at the data centre service provider is monitored using a network infrastructure monitoring tool, which reports any servers which are "unreachable devices". Should any servers be identified as an unreachable device, then a call is logged in Service Now in order for the matter to be resolved. A report run on 1 April 2019 showed there were no exceptions. The Service has advised other tools are in place to help maintain the confidentiality, availability and integrity of Council data.

2.7.3 The Cluster also receives monthly Service Reports and Additional Service Report Information, from the data centre service provider, which detail: individual servers failing the Service Level Agreement availability of 99.9%; change requests; "red" server capacity alerts (meaning servers are reaching their capacity limits); managed server restores; number of requests by Council staff to access the data centre; project updates e.g. disaster recovery testing; the operational risk register (used to monitor any ongoing risks), and storage use and costs. The January, February and March 2019 reports all showed overall server availability met the 99.9% SLA target.

2.7.4 The Council is part of the Scottish Wide Area Network (SWAN), a network designed to be secure to facilitate data sharing and collaboration within the public sector. The SWAN portal enables D&T to monitor the availability of connections to Aberdeen City Council remote sites, with each site listed and the connection status reported on the portal as green, amber or red, depending on performance. This enables D&T to monitor the availability of network connections. If a site is reported as amber or red then a Desktop Analyst attends the site to determine the nature of the fault, with a call raised with SWAN to resolve the matter, if it cannot be resolved locally. A SWAN report as at 8 April 2019 showed all Council live sites were green, indicating connection status was adequate.

2.7.5 SWAN will also proactively identify network outages and escalate these to the Council, including during out of hours.

2.7.6 Should any of the Council's business critical system servers cease to operate at the data centre provider or any of the servers used by the Council reach their predefined storage use warning thresholds, a critical 1 call is automatically raised by the data centre provider on Service Now. In order for appropriate corrective action to be taken by D&T. Service Now tickets had been raised for 153 such instances since April 2018. D&T advised these had been resolved as indicated by the priority being graded at 2 (high) or 3 (moderate) as at 1 April 2019 (as opposed to 1 critical). For a sample of calls reviewed appropriate action had been taken.

2.7.7 A sample of cloud-based suppliers, used to manage Council data, were reviewed to ensure the Council had access to a service call function for logging performance issues and that the supplier was reporting on contractual system key performance indicators.

2.7.8 The Customer Experience Platform specifies the minimum system availability and the target response times for addressing system faults based on the level of disruption to system functionality. System performance issues, including those relating to system availability, can be logged and progress resolving these calls can be monitored, using the customer support portal provided by the supplier.

2.7.9 Comprehensive performance reporting was being provided for the Planning Consultation System in accordance with the SLA.

2.7.10 It was not possible to determine if the supplier was reporting on KPIs for the Early Years Admission and Enrolment System, since the contract was unavailable (recommendation included at 2.4.5).

Recommendation
Assurance should be gained over contractually agreed performance for the Early Years Admission and Enrolment System.

Service Response / Action
Early Years Admission and Enrolment System – Agreed.

Implementation Date	Responsible Officer	Grading
July 2019	Early Years Manager	Important within audited area

2.8 Governance

2.8.1 The purpose of the Information Governance Group is to support and drive the broader information governance agenda, provide the Corporate Management Team (CMT) with assurance that effective control mechanisms are in place, and manage and mitigate the Council's information risks. The Group provides a quarterly report to CMT on Information Governance Management and an annual report to the Audit, Risk and Scrutiny Committee, as referred to in paragraph 2.2.2. These reports include a section on cyber security risks, covering the number of incidents and attempts threatening the Council's information, software, infrastructure or computer network, that originate from inside and outside the organisation.

2.8.2 The 2018/19 quarter 3 performance report was reported to CMT on 28 February 2019 and the annual report for July 2017 to June 2018 was discussed and noted by the Audit, Risk and Scrutiny Committee on 25 September 2018.

2.8.3 The Security Team prepares a monthly ICT security report for D&T senior management. This includes various statistics including: web risks prevented; email traffic; IT risk register status; and, an update on the operational risks of high importance. Both the January and February 2019 reports had been issued to D&T management by the Security Team as expected.

AUDITORS: D Hughes
A Johnston

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.