ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	27 September 2022
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2111 – Building Maintenance System
REPORT NUMBER	IA/AC2111
DIRECTOR	N/A
REPORT AUTHOR	Jamie Dale
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 the Building Maintenance System

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 the Building Maintenance System.

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 Council Delivery Plan, or the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place.

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
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

9. APPENDICES

9.1 Internal Audit Report AC2111 – Building Maintenance System

10. REPORT AUTHOR DETAILS

Jamie Dale, Chief Internal Auditor
Jamie.Dale@aberdeenshire.gov.uk
(01467) 530 988

Internal Audit Report

Operations

Building Maintenance System

Issued to:

Rob Polkinghorne, Chief Operating Officer
Steven Whyte, Director of Resources
Andy MacDonald, Director of Customer Services
Gale Beattie, Director of Commissioning
Mark Reilly, Chief Officer - Operations
Steve Roud, Chief Officer – Digital and Technology
Craig Innes, Head of Commercial and Procurement
Fraser Bell, Chief Officer – Governance
Jonathan Belford, Chief Officer – Finance
John Noble, System Support Manager
Helen Cannings, Data Protection Officer
External Audit

Date of Issue: July 2022 **Report No. AC2111**

EXECUTIVE SUMMARY

Background
The building maintenance system is a package of software used to manage, report on, and deliver reactive and scheduled property repairs to council tenants and other service subscribers. It also covers void property work and inspections, job ticketing, scheduling, invoicing, stores management (depots and tradesmen's vans), purchase ordering, creditor payments and alerts.

During 2021/22 the system administered 136,482 repair jobs and raised 30,446 purchase orders totalling £25.456 million.

Objective
The objective of this audit was to provide assurance over system controls, including access controls, system security and backups, interfaces, business continuity and contingency plans.

Assurance
In general there is assurance over system access and training, and there are business continuity and contingency plans in place. Risks have been highlighted in respect of application of best practice and Council policy in system access, use and security arrangements, which the Service will explore with the supplier as part of a planned upgrade project.

Findings and Recommendations
On 1 April 2022 the Council relicensed the system, which will include an upgrade and hosting on the supplier's cloud, at a cost of £405,390 over two years, with an option to extend for a further 12 months thereafter. The Council's procurement regulations were suspended with approval from the Director of Commissioning, and Scottish Procurement Regulations were not applied, to allow a direct award in excess of local and national cost thresholds, justified as *"urgently required to meet the exigencies of the Function/Cluster"*. However, the original contact with the supplier had already lapsed in 2019/20 and a suspension of Procurement Regulations sought and granted for the financial year 2020/21. A further extension was undertaken for the financial year 2021/22 without obtaining written approval for suspending procurement regulations. This indicates a lack of forward planning, and a risk to achieving best value. A recommendation graded Significant within audited area has been made to ensure procurement is adequately planned to ensure transparency and avoid the need to suspend procurement regulations.

Supplier access agreements are out of date, and data protection risks have not been subject to review. Recommendations graded Significant within audited area have been made to update access and data sharing agreements and conclude a data protection impact assessment for the upgraded system.

System password controls and access restrictions do not currently meet the Council's standards, and there is no process for reviewing ongoing user access requirements e.g. where users have left or changed jobs. Recommendations graded Significant within audited area have been made to ensure the system reflects the Council's security requirements, and to implement an annual user access audit.

Assurance over use of the system may be affected because of the use of a number of generic usernames for particular activities, and a need for a small number of processing users to use system administrator roles to complete some transactions. This impacts on the effectiveness of transactional controls and the audit trail of user activity. Recommendations graded Significant within audited area have been made to limit use of generic users and to review the processing requirements with the supplier.

It should be noted that there are currently plans for Service redesign where the team responsible for managing the system in Building Services may be transitioned from Building Services to Digital and Technology. This may impact on the reporting of actions in the future and will be monitored by Internal Audit.

Management Response
Whilst the system was not open-market tendered, it has now gone through the Council's Procurement Governance process appropriate to direct awards.

Supplier access arrangements will be reviewed, and data protection risks formally considered and documented.

Options for adjusting system parameters to reflect the Council's password and workflow requirements may be limited but this will be explored with the supplier as part of the upgrade project.

There is insufficient resource within the system support team to carry out annual user audits, however we will liaise with D&T regarding options to incorporate into the corporate D&T leavers process.

The current record of assigned generic users has been reviewed to ensure all are still appropriate. The technical issues requiring such users will be raised with the software supplier as part of the system upgrade.

11. INTRODUCTION

11.1 The building maintenance system is a package of software used to manage, report on, and deliver reactive and scheduled property repairs to council tenants and other service subscribers. It also covers void property work and inspections, job ticketing, scheduling, invoicing, stores management (depots and tradesmen's vans), purchase ordering, creditor payments and alerts.

11.2 During 2021/22 the system administered 136,482 repair jobs and raised 30,446 purchase orders totalling £25.456 million.

11.3 The objective of this audit was to provide assurance over system controls, including access controls, system security and backups, interfaces, business continuity and contingency plans.

11.4 The factual accuracy of this report and action to be taken regarding the recommendations made has been agreed with, John Noble, System Support Manager, Steve Roud, Chief Officer - Digital and Technology and Helen Cannings, Data Protection Officer.

12. FINDINGS AND RECOMMENDATIONS

12.1 Written Procedures

12.1.1 Comprehensive written procedures that 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, especially in the event of an experienced employee being absent or leaving.

12.1.2 The Systems Development team (System team) has written procedures covering all team tasks. These are maintained on SharePoint and are accessible to all staff who require them. Procedures are reviewed whenever a system update is carried out and when new staff are being trained, to ensure they are current.

12.1.3 Along with written procedures, new staff will only be given access to the 'live' system after they have received training from line managers and peers within the transactional teams. This training is carried out on a test database as well as 'live' within the system.

12.2 Contracts

12.2.1 On 1 April 2022 the Council relicensed the system, which will include an upgrade and hosting on the supplier's cloud. The Chief Officer Digital and Technology received approval from the Director of Commissioning to undertake a direct award to the framework supplier in accordance with the Council's Scheme of Governance. The contract is for a two-year period with the option to extend for 12 months.

12.2.2 The estimated cost for the contract including support and maintenance was set out on a procurement business case as £161,000 per annum, or £322,000 over two years. However, the contract is logged on the contracts register at a value of £237,928. The contract itself sets out an annual fee of £165,389, plus further fees of £2,073, and one-off charges of £59,067 and £11,399. Further costs may be incurred at a pre-agreed rate for additional services. The base cost of the contract over two years is therefore £405,390, and £572,852 if the extension is taken up.

12.2.3 The request for the suspension of Aberdeen City Council procurement regulations 2021 3.10 indicated regulation 4.4.1 was being suspended - where a contract has an estimated value of between £50,000 and the higher threshold limit. However, the value of this contract exceeds the higher value threshold as published by the Scottish Government for public contracts of £213,477. The contract value listed on the request was £483,000. The request for suspension should therefore have referenced procurement regulation 4.5.1, and non-adherence to Scottish Procurement Regulations. The procurement has yet to be notified to the Strategic Commissioning Committee as required under council procurement regulation 3.11.

12.2.4 The suspension was justified as *"urgently required to meet the exigencies of the Function/Cluster*". However, the original contact with the supplier had already lapsed in 2019/20 and a suspension of Procurement Regulations sought and granted for the financial year 2020/21. A further extension was undertaken for the financial year 2021/22 without obtaining written approval for suspending procurement regulations. The fact a further request to suspend the regulations has been asked for appears to indicate either a lack of forward planning or deliberate choice to not open the contract to the market. Without going out to the market there is a risk of not obtaining best value from an appropriate digital solution.

Recommendation

a) The Service should ensure appropriate forward planning is undertaken so as not to require suspension of Procurement Regulations, and to ensure costs and approvals are accurate and fully transparent.

b) The Service should ensure the contract, including the reason for suspending local and national procurement regulations, is reported to the Strategic Commissioning Committee.

Service Response / Action

a) Service attempted to bring up to date in 2020 but due to Corporate Digital Review any decisions on this system were put on hold. System has now gone through the Procurement Governance process, although not an open market process which has resulted in an extended three year contract. This is an upgrade to the current system as opposed to a completely new system, this will ensure that the service has a streamlined transition from the current system to the new upgraded cloud based system.

b) Reasons will be included in a Register of approved memos prepared by Commercial and Procurement which is reported along with each cycle's Workplans and Business Cases. The next report will be submitted to Committee in September 2022

Implementation Date	Responsible Officer	Grading
a) September 2023	Operations Manager	Significant within audited area
b) September 2022	Strategic Procurement Manager	

12.2.5 All external parties who require access to Council systems are required to complete a 'Third Party Access Registration form" before access is granted. This form sets out the details of who requires access, the level of access and reason. It also sets out the roles and responsibilities of both the Council and the third party to ensure the system data is protected. Access to the system databases and applications / modules is provided via a VPN (Virtual Private Network). A third-party access registration form was last signed in 2016 by the Council and the system support and maintenance contractor and is out of date as it refers to systems and processes no longer in use.

Recommendation

An up to date third party access agreement should be completed for the revised system.

Service Response / Action

The current access agreement will be re-assessed and updated to reflect the current position.

Implementation Date	Responsible Officer	Grading
July 2022	Infrastructure Architect	Significant within audited area

12.3 Data Protection

Data Processing Agreement

12.3.1 GDPR Article 28(3) and section 59(5) of the Data Protection Act 2018 require where a data controller such as the Council uses a Data Processor to process personal data on its behalf, that the processing 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 and the processor.

12.3.2 GDPR Article 28 goes on to state the contract shall stipulate that the processor: only processes the personal data concerned on documented instructions from the Controller, including with regards to transfers of personal data to a third country or international organisation; the persons authorised to process the personal data have committed themselves to confidentiality; appropriate technical and organisational measures are put in place by the processor to protect personal data; personal data will be deleted or returned to the controller at the end of the provision of services relating to processing; and the processor will allow for and contribute to audits by the controller or another auditor mandated by the controller.

12.3.3 With the extension to the system license the revised contract contains the required documentation to cover the requirements of a data processing agreement.

Privacy Notices

12.3.4 In accordance with GDPR Article 13, where personal data relating to a data subject is collected, the Council uses privacy notices to: explain the purposes of processing; the legal basis for processing; the data subject's rights in relation to their personal data held by the Council; whether the data will be shared with any other parties; whether there is any automated decision making or profiling using the personal data; the retention period; and the contact details of the Data Protection Officer responsible for monitoring the Council's compliance with Data Protection legislation.

12.3.5 The Privacy Notice must provide information to individuals in a concise, transparent, intelligible, and easily accessible way and must be written in clear and plain language. The Council publishes all its privacy notices on its website. As the system is used to process property details along with the associated tenants' personal data a privacy notice under Housing Repairs has been published on the Councils website.

12.3.6 As indicated in paragraph 2.3.4 above, in accordance with the GDPR, privacy notices must provide details of how long the Council will hold a customer's personal data for. The Housing repairs privacy notice indicates "The record of the repair to the property will be stored electronically and will be kept as long as the property exists and remains in council ownership. At the end of this period it will be securely destroyed." Details of the property would not be viewed as personal data however it does not indicate whether any of the tenants' details are retained for this length of time. On this basis any property which is sold or demolished should be removed from the system, there would also be a question regarding data held for mutual repairs, where home-owners may have been included with any works undertaken.

12.3.7 When the system team was asked whether the retention period was being adhered to, they indicated no records had ever been archived from the system and they were unsure whether the current version of the system could distinguish between different property types to enable automatic archiving/deletion of certain records. Following Internal Audit's enquiry, the system team undertook an extract of properties which were no longer owned by the Council and held personal details of the former tenants. This showed 2,030 records which held the former tenant's name. The system team has undertaken a tidy up of these records and has removed any personal data.

12.3.8 Data is also held in a Test version of the database, which is only updated as and when required to support and test changes and upgrades. Any personal data held in this part of the system may therefore not comply with the GDPR requirement to maintain it accurately and up to date.

Information Asset Register

12.3.9 Article 30 of the GDPR specifies data controller record requirements relating to processing activities. The Council achieve this by way of an Information Asset Register (IAR) arranged in four parts by Information Asset Owner Register, Register of Data Flows, Register of Systems/Wrappers, and Register of Processing Activities. The building maintenance system is recorded on all parts of the IAR.

Data Sharing

12.3.10 A summary of the privacy notices published on the Council's website indicates personal data that the Council controls is shared with third party contractors who may undertake the repair work.

12.3.11 Section 5.4 'Information Sharing Protocols and Agreements' of the Council's Managing Information handbook covers the requirements when personal data is shared with another Data Controller, stating:

"Any disclosure or sharing of personal data will be carried out in accordance with Data Protection law. Where data sharing is routine, i.e. more than ad-hoc, a Privacy Impact Assessment [otherwise known as a Data Protection Impact Assessment] shall be undertaken, and a Data Sharing Agreement or Information Sharing Protocol shall be put in place between parties to the agreement".

12.3.12 The exception is External Audit, who are entitled to system access, in accordance with section 100 of the Local Government (Scotland) Act 1973, Auditor's right of access to documents. Where the Council shares personal data with a Data Processor, a Data Processor Agreement is required as per paragraph 2.3.1 above.

12.3.13 For new systems or data processing proposals, information gathered as part of the Council's Data Protection Impact Assessment (DPIA) process provides the basis for drafting an appropriate Data Sharing Agreement. The DPIA should be reviewed by the Information Asset Owner (third tier manager) and Data Protection Officer. There is no DPIA in place for the Building Maintenance system, as this system has been in place since 2001. The contracted upgrade to the system, which includes the move from Council controlled Servers to the contractors hosted Cloud could be viewed as a significant change to the way tenant data is being handled, and in such a case a DPIA would be appropriate to identify and address any potential risks.

12.3.14 A review of the third party Data Processors and Controllers with whom personal data held in the System is shared found a current data processing agreement was not in place with the Council's third party repairs contractors. Carrying out a Data Protection Impact Assessment of the Building Maintenance system will facilitate this process, by identifying personal data being shared with third parties and the related risks.

Recommendation

Customer Experience should assess the data protection risks associated with the Building Maintenance system and use this process to ensure appropriate data processing agreements and data sharing agreements are in place.

Service Response / Action

The system upgrade will incorporate works to ensure all measures are in place to fully comply with all risks associated with Data protection.

Implementation Date	Responsible Officer	Grading
September 2023	Operations Manager	Significant within audited area

12.3.15 Section 3.2 'Confidentiality and you" of the Council's Managing Information handbook covers the requirements of dealing with confidential personal information. It emphasises a Council employee's contract of employment covers their duty of confidentiality. Except for the support and maintenance contractor, for which confidentiality is covered in the contract, non-council employees do not currently access the system.

12.4 Timetabling of Milestone Events

12.4.1 The System team maintains a detailed timetable for all database maintenance and routine processes that require to be run throughout the year. The timetable is prepared prior to the start of the new financial year with daily, nightly, weekly, two-weekly, four-weekly, and yearly tasks to be completed detailed e.g. (changes to the schedule of rates); Certain jobs are scheduled to run within the system while the majority rely on users having completed processes before a job can be run by members of the system team. Currently there is no checklist for the systems team to indicate the required job has been undertaken. This presents a risk of jobs not being undertaken, potentially impacting on subsequent processes. The Service have indicated the only critical process is the nightly interface to e-financials to ensure suppliers are paid timeously. This process produces control emails notifying the systems team should the process fail. There are also controls at the e-financials end where Finance staff undertake checks of the files being loaded.

12.5 System Parameters

12.5.1 Changes to system parameters, such as schedules of rates (SORs), can only be completed by staff in the System team. Changes to system parameters are tested primarily on the Test system before being put onto the Live system, and a full audit trail is produced by the Service. System parameters are changed mainly at the request of the Service.

12.5.2 A review of the update to the SORs for 2021/22 found they had been supplied by the Service, updated, and checked by the systems team and the Service prior to going live.

12.6 System Access, Security and Audit Trails

Access

12.6.1 System access is requested by email from a line manager. The emails normally provide the job role the employee is to fill, or a reference to another current member of staff already in a similar position. The employee's access to the system is determined by their post, with different "access groups" for the different responsibilities, i.e. storeman, tradesman, invoice processor etc.

12.6.2 When an employee is going to leave the Council, for their system account to be closed, the System team must receive a request through IT or from the employee's line manager. A review of all current users on the system was compared to leavers recorded through the Council's payroll system between January 2017 and January 2022 and this identified eight users who had left the Council but were still "live" users in the system. The current system does not lock users from the system after any period of non-use. The users were notified to the System team to check and correct.

12.6.3 While the process for notifying the System team is not linked to the Council's leavers process, the Council's leavers process does ensure IT are notified, and access to the Council's networks is removed. Without a Council login it is not possible to access the system, reducing the risk of unauthorised access by former employees. However, it was confirmed with Digital & Technology (D&T) that current security settings would mean those with web client access would still be able to access the system using their own device. D&T indicated this should be addressed with the upgrade to the new system.

12.6.4 The System does not log out users who have been inactive within a live session for a certain amount of time where they are using the desktop client, but it does log out users using the web client after 20 minutes. An extract of live system users indicated 95 had never logged onto the system. The Systems Team indicated these users may only be using the TotalView front end of the system and their log on data may not be recorded on the audit trail. The fact the system does not lock users after periods of inactivity poses a risk of such staff still being able to access the system in the future, even though their job role may have changed. A record of these users was provided to the systems team to ascertain whether access should be removed entirely.

Recommendation

The Service should explore options to lock users after a set period of inactivity with the software provider as part of the system upgrade.

Service Response / Action

Agreed. The Business & Systems Support Manager will raise this with the software provider to ascertain if this can be applied in the current system. It will also be looked to be addressed as part of the system upgrade.

Implementation Date	**Responsible Officer**	**Grading**
August 2022.	Business & Systems Support Manager	Significant within audited area

12.6.5 Where a member of staff changes post within the Council, line manager notification to the System team is required to remove / amend system access. On 28 February 2022 there were 330 live users, with 75 job titles across all Council Functions.

12.6.6 Three staff with Administrator access were found in the review, these staff do not form part of the system team. The reason for these staff having administrator profiles was raised with the Operations Development & Performance Officer who indicated this was because of the tasks two of the users required as part of their job roles as part of a costing process. The current system profiles only allow this to be undertaken as part of the administrator profile. The third user had previously undertaken this task; however they have now moved job, therefore their profile should be updated. Having transactional staff with administrator access poses control issues under segregation of duties. Such issues with profile construction should be raised as part of the system upgrade.

Recommendation

The system team should raise the issue of transactional processes only being available under an administrator profile as part of the system upgrade.

Service Response / Action

Agreed. The current system does not allow for this differentiation but will be raised as part of the system upgrade project.

Implementation Date	**Responsible Officer**	**Grading**
September 2023	Business & Systems Support Manager	Significant within audited area

12.6.7 The issues in the preceding paragraphs indicate a lack of control over user management within the system, due to the lack of a corporate leavers process which would alert the systems team to changes required to system users. Without this process a possible solution is an annual review of users, with line managers being contacted to provide confirmation that users are still current and have the correct level of access to the system to carry out their job.

Recommendation
The System Team should carry out an annual audit of users to ensure they still require the access they hold.

Service Response / Action
Due to resource issues within the system team such a review would not be feasible. We would prefer to cover under the leavers process, through the notification to D&T. We will contact colleagues in D&T and ascertain if this is possible.

Implementation Date	**Responsible Officer**	**Grading**
July 2022	Business & Systems Support Manager	Significant within audited area

Passwords

12.6.8 The Council's Password Standard requires user passwords to be at least eight characters long while system administrators' should be fifteen. Both should contain three of the required categories: upper case, lower case, numbers, or special characters. Currently neither the user nor administrator passwords comply with the standard. The user passwords do not require the three categories but do require to be eight characters long. The administrator passwords currently mirrors the user password requirements. The systems team believe the current system parameters do not allow variations in character length. Compliance with the Council's password standard should be investigated with the introduction of the new system upgrade.

Recommendation
The System Team should ensure the system enforces compliance with the Councils password standard.

Service Response / Action
Agreed. Current system does not provide this functionality, but it will be raised as part of the system upgrade.

Implementation Date	**Responsible Officer**	**Grading**
September 2023	Business & Systems Support Manager	Significant within audited area

12.6.9 The system locks user access following three failed login attempts. Users must email the System Team to have it unlocked. There is no requirement for the unlocking to be authorised by a line manager.

Audit Trails

12.6.10 The audit trail functionality cannot be disabled in the system. However, the timescale for which the various changes are recorded in the system differs, e.g. a purchase order approval structure overwrites the previous structure, while the SOR changes maintains a full history of all changes. The functionality of the audit facility is dictated by the system.

12.6.11 The system has 23 generic user profiles – i.e. accounts set up not linked to any single specific user. Six of these are system required, for the maintenance and support provider to access on request or to allow interfaces to run automatically. The remainder have been set up as a work-around for technical variations between the system and service setup – for example standard access rights do not permit purchase orders to be edited and re-approved. The system team maintains a spreadsheet showing who was given access but not when it was removed / ended.

12.6.12 These accounts present a risk, as it may not be possible to attribute transactions or changes to an individual officer and hold them to account in the event of an error. Moving to a new version of the system could present an opportunity to improve alignment with service requirements. If generic users are still required, their use needs to be effectively controlled and monitored.

Recommendation

The Service should ensure system access is aligned with service requirements, and that use of generic users is limited and monitored.

Service Response / Action

Agreed. The current record of assigned generic users has been reviewed to ensure all are still appropriate.
The technical reasons requiring such users will be raised with the software supplier as part of the system upgrade.

Implementation Date	**Responsible Officer**	**Grading**
September 2023	Business & Systems Support Manager	Significant within audited area

12.7 System Testing and Development

12.7.1 To enable the Service to test database upgrades, amendments, and fixes before applying them to the Live database, a Test database is available. The Test database mirrors the Live database and is populated with the data held on the Live database to give staff the ability to fully test any changes prior to being applied to the Live database

12.7.2 The latest system upgrade in April 2020 changed the operating database from oracle to SQL. The systems team undertook a series of tests within both the test and live database to ensure the expected outcomes for the processes within the system remained constant. Records of the tests, results, and any follow up of errors/anomalies was maintained.

12.8 Interfaces & Reconciliations

12.8.1 The System team administers the interfaces to and from, and within the system, and these are fully documented. The principal system interfaces are:

From

- Operational Buildings Management System – job requests, as and when jobs are raised
- HRA Housing Management system – Property status and tenant information updates, updated daily.

To

- Financial – Creditors system for supplier invoices to be paid, updated daily.
- Operational Buildings Management System – confirmation of stages of each job, request receipt, attendance at site and completion details, updated hourly. Internal charging for completed jobs, monthly.

12.8.2 Should an interface fail, or have individual rejections within a file, the system team is notified by email automatically by the system. One month's interfaces were tested for each of the systems, except for the Creditors' interface which was tested as part of the Financial System Interfaces audit, report AC2209. Testing found no files had failed entirely and where any rejections were reported, these were found to have been intended for external contractors – and therefore should not have been processed on the system, showing the interface correctly identifies such errors. There are no reconciliations between systems.

12.9 Contingency Planning and Disaster Recovery

12.9.1 The Building Services business continuity plan is detailed, covering all the business functions, although the appendices, including the key supplier assessment questionnaire (which assesses supplier ability to continue providing services in event of major incident affecting supplier operations) were not completed as required. The plan is currently under review in consultation with the various stakeholders. The omission of the appendices has been highlighted to the project lead for addressing.

12.9.2 Files are backed up by the Council's data centre service provider in full on a weekly basis and incrementally daily, with 30 days of backup files held locally and a 90-day offsite retention held in the disaster recovery datacentre in another location. The Service Level Agreement with the data centre service provider specifies in the case of outages, service should be restored within 24 hours and a permanent fix applied within two days to prevent recurrence. Daily system backups are scheduled. Logs for October 2021 demonstrated that backups had been completed for each of the nights. However, it was noted a number of the backups had been completed "with errors". Digital and Technology clarified that this relates to system files / directories being open at the time of backing up, however the backups still completed successfully, and this does not impact on the reliability of the data or the ability to retrieve data from them.

12.9.3 The system is deemed a business critical system and as such it appears on the schedule of disaster recovery testing. The resilience test for 2021 was delayed due to a technical issue resulting in a failed test. This will be planned for early 2022 once the cloud modernisation project has completed. However, D&T indicated the system is replicated to the Councils disaster recovery datacentre and if the Aberdeen Data Centre became unavailable D&T would invoke the contingency for this system with a Recovery time objective of two hours.

12.10 Database Performance

12.10.1 The system is pivotal in the maintenance process for Council housing and operational buildings along with timeous payment of suppliers. As such it is vital the database operates at an optimum level and is available for use. The Systems Development Officer indicated downtime, outwith scheduled upgrades, is almost zero (three in 12 months, two of which were for less than 10mins, the other four hours). As at 28 February 2022 there were no open calls with the support and maintenance provider

AUDITORS: J Dale
C Harvey
G Flood
C 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.