CARLISLE
CITY COUNCIL
www.carlisle.gov.uk

Audit of Smarter Service Delivery

Draft Report Issued:	**18 July 2018**
Director Draft Issued:	**07 August 2018**
Final Report Issued:	**09 August 2018**

Audit Report Distribution

Client Lead:	Customer Services Manager
Chief Officer:	Chief Executive
Others:	Service Improvement Officer Lead ICT Officer (T1094) Lead ICT Officer (T1095) Senior ICT Officer (T1102) Information Governance Manager
Audit Committee:	The Audit Committee, which is due to be held on 26th September will receive a copy of this report.

Note: Audit reports should not be circulated wider than the above distribution without the consent of the Designated Head of Internal Audit

1.0 Background

1.1. This report summarises the findings from the audit of the Smarter Service Delivery project. This was an internal audit review included in the 2018/19 risk-based audit plan agreed by the Audit Committee on 19th March 2018.

1.2 Smarter Service Delivery is a long-term project being undertaken by the City Council to increase digital usage by City Council service users.

1.3 The project is underpinned by the transition of business processes to Salesforce, a customer relationship management software package. Numerous Council Services including Waste Services, Green Spaces and Environmental Health have been transitioned and are now processed using Salesforce.

1.4 In addition, Salesforce can be used for other aspects of business processes (e.g. stock control) and the Council is looking to expand the use of the software, modernising service delivery across the full Council.

2.0 Audit Approach

Audit Objectives and Methodology

2.1 Compliance with the mandatory Public Sector Internal Audit Standards requires that internal audit activity evaluates the exposures to risks relating to the organisation's governance, operations and information systems.

2.2 A risk-based audit approach has been applied which aligns to the five key audit control objectives (see section 4). Detailed findings and recommendations are reported within section 5 of this report.

Audit Scope and Limitations.

2.3 The Audit Scope was agreed with management prior to the commencement of this audit review. The Client Lead for this review was the Customer Services Manager and the agreed scope was to provide independent assurance over management's arrangements for ensuring effective governance, risk management and internal controls of the following scope areas:

- Risk 1. Failure to achieve business objectives due to insufficient governance
- Risk 2 Loss of or failure to secure sensitive personal information and comply with data protection legislation, resulting in sanctions and reputational damage.
- Risk 3 – Implementation of Smarter Service delivery does not achieve intended objectives (e.g. an easier to access, more efficient service).
- Risk 4 – Failure to successfully implement Smarter Service delivery due to lack of buy-in from service providers.

2.4 There were no instances whereby the audit work undertaken was impaired by the availability of information.

3.0 Assurance Opinion

3.1 Each audit review is given an assurance opinion and these are intended to assist Members and Officers in their assessment of the overall level of control and potential impact of any identified system weaknesses. There are 4 levels of assurance opinion which may be applied. The definition for each level is explained in **Appendix B.**

3.2 From the areas examined and tested as part of this audit review, we consider the current controls operating within Smarter Service Delivery provide **Reasonable assurance**.

Note: as audit work is restricted by the areas identified in the Audit Scope and is primarily sample based, full coverage of the system and complete assurance cannot be given to an audit area.

4.0 Summary of Recommendations, Audit Findings and Report Distribution

4.1 There are two levels of audit recommendation; the definition for each level is explained in **Appendix C**.

4.2 There are 5 audit recommendations arising from this audit review and these can be summarised as follows:

Control Objective	High	Medium
1. **Management** - achievement of the organisation's strategic objectives achieved (see section 5.1)	-	-
2. **Regulatory** - compliance with laws, regulations, policies, procedures and contracts (see section 5.2)	-	1
3. **Information -** reliability and integrity of financial and operational information (see section 5.4)	1	3
Total Number of Recommendations	**1**	**4**

4.3 Management response to the recommendations, including agreed actions, responsible manager and date of implementation are summarised in Appendix A.

4.4 **Findings Summary (good practice / areas for improvement):**
There is a thorough governance framework in place to monitor delivery of the project, with regular financial, performance and risk monitoring in place. The Project's outcomes are well defined and progress is monitored by both Senior Management and Members. There is a strong understanding of roles and responsibilities within the team.

Suitable documentation is in place for each sub-project, which are delivered in line with the Council's Project Management procedures. Service providers are consulted throughout the process and demonstrated satisfaction with the support provided during transition to the new software.

In order to quantify the success of each sub-project it is suggested that performance of the perceived benefits identified at the start of the project are measured following completion. This information can then be used to learn lessons for future transitions to the Salesforce software.

Four recommendations have been made in relation to records management, particularly with regard to compliance with the new data protection legislation (GDPR).

There is currently no system in place to archive and delete personal information retained within the Salesforce and My Account software packages and users are currently not required to give consent to the use of their data (a requirement of the new legislation). In addition, there is a need for some officers to complete mandatory information governance e-learning introduced by the Council.

In addition, security of the data held in My Account could be improved by strengthening password requirements.

Comment from the Chief Executive

Thanks to Internal Audit. I am pleased to note that the recommendations will be implemented before the end of August.

5.0 Audit Findings & Recommendations

5.1 Management – Achievement of the organisation’s strategic objectives

5.1.1 The Smarter Service Delivery Project is listed as a key priority within the Customer Services Service Plan for 2018/19.

5.1.2 A cross-departmental team (Customer Services and IT Services) is in place to manage delivery of the project. The team demonstrated a clear awareness of their responsibilities within the project and suitable reporting structures and clear, up to date job descriptions are in place.

5.1.3 The Chief Executive is the Senior Management Team member with responsibility for overseeing delivery of the project. The Chief Executive chairs the Transformation Board, which receives regular updates on progress against the project. Progress is also reported to Members via the Business Transformation Scrutiny Panel.

5.1.4 Performance monitoring is in place to measure the take-up of digital services, including a Performance Indicator (as part of the Council’s Corporate Performance Monitoring Framework) to measure the percentage of online service requests. The Transformation Board also receives regular updates to the number of on-line accounts registered by residents.

5.1.5 At the time of review, a target had not been set for the 2018/19 performance indicator. As the previous year’s target was achieved, Internal Audit advise that any target set for the current year aims to continually improve services (i.e. is greater than the previous year’s target).

5.1.6 The Customer Services Manager also prepares a series of detailed performance dashboards to monitor overall usage of Salesforce, including the extent of digital services being utilised.

5.1.7 Financial performance is monitored on a regular basis, with no concerns arising.

5.1.8 Risks are reviewed by the Customer Services Manager on a regular basis, who has recently added a new risk to reflect the introduction of the new Data Protection legislation in March 2018 (See section 5.3).

5.1.9 Discussions with the Customer Services Manager indicated a good understanding of the risks faced by the project and suitable mitigating strategies are in place. Guidance was provided during the audit to ensure risks are formally documented as having been reviewed with Project Server (the Council’s Risk Monitoring software).

5.2 Regulatory – compliance with laws, regulations, policies, procedures and contracts

5.2.1 The core role of the Project Team is to oversee the transition of Council Services onto Salesforce.

5.2.2 The Council replaced the previous Customer Resource Management tool with Salesforce, which is now used by Customer Services to process all queries and direct service requests.

5.2.3 Service delivery is now also being transitioned to Salesforce (via a series of sub-projects), so that the full business process is contained within the software. Green Spaces, Waste Services and Pest Control have already been transitioned and the team are currently in the process of transitioning Enforcement.

5.2.4 Individual sub-projects are managed using the Council's Project Management methodology, which has a defined procedure in place for both large and small projects (depending on a scoring process based on the perceived size and complexity of the project).

5.2.5 A review of a sample of sub-projects indicated suitable business cases are documented, with project outcomes clearly defined from the onset. However, it was found the project scoring was not visible; it is advised this information is retained within the business case documentation (to ensure transparency of the process).

5.2.6 The Service Improvement Officer works closely with the Service Provider to understand and review existing processes, including determining if any efficiencies or improvements can be made to the process. IT Services then develop modules within Salesforce to ensure processes can be delivered in line with service provider and service user requirements.

5.2.7 Project Documentation, including meeting notes, user acceptance testing and an audit trail of work done by the IT team is retained within 'Confluence', an online repository used to aid the Project Management process. Suitable documentation was held on file for the sample of projects reviewed.

5.2.8 Feedback from Service providers indicated they were satisfied with the level of support and guidance received both throughout and after the transition period. The only area of concern raised relates to the level of resource available. It was identified that a member of IT services responsible for developing Salesforce modules is vacating their post. It is advised that resource levels are reviewed, to ensure the level of support provided to service users is not compromised.

5.2.9 At the start of each sub-project measurable benefits (e.g. an increase in online applications) are identified that are expected to be realised following completion of the transition.

5.2.10 To date, there has been no measurement of these potential benefits following full implementation of a new service.

5.2.11 Obtaining this performance data would give insight into which perceived benefits have been realised and which have not. These findings will act as valuable information for the transition of future services.

Recommendation 1 – Following project completion, measurements should be taken to determine if perceived benefits outlined at the project's onset have been realised.

5.3 Information – reliability and integrity of financial and operational information

5.3.1 Sensitive personal information is retained in both My Account (an application within the Council's internet site, used to allow residents to create online accounts) and Salesforce.

5.3.2 A document retention schedule is in place, listing the type of information held within each system. There is currently no specified retention periods for the information retained, nor is there a process to archive or delete records within either system.

5.3.3 Both systems are relatively new and therefore currently do not contain out of date information, therefore the current risk exposure is considered medium.

5.3.4 It is still imperative an archiving and deletion process is established to ensure personal information no longer required by the authority is deleted (for example, customer accounts that have not been used for a number of years should be considered for deletion). If this issue is not addressed the Council will eventually be holding out of date and unnecessary personal information, resulting in a breach of data protection legislation (therefore increasing the risk exposure to high).

Recommendation 2 – A process should be developed to archive and/or delete personal information held within both Salesforce and My Account, in line with suitable retention periods.

5.3.5 The new data protection legislation requires individuals to consent to the use of their personal data. This consent must be clear, cover all uses and must not be enticing.

5.3.6 While the Council has a suitable privacy notice in place on it's website, at the time of the audit there is no process in place for service users registering an online account with the Council to consent to their date being used.

Recommendation 3 – A consent notice should be implemented within My Account that requires all registered users (both new and historic) to give consent to their personal information being used by the Council.

5.3.7 Data within My Account is held on the Council's servers and therefore protected by the Council's firewall security. Access to this information within the Authority is restricted to the relevant Administrator.

5.3.8 Public access to individual accounts is restricted by a series of security facilities including password control, e-mail verification and security questions. In addition, further verification (such as providing a bill reference) is required for an individual to request services.

5.3.9 The current requirements for the application's password facility was found to be at the lowest security level (no combination of letters, numbers or special characters required). There is an option within the system to enforce system users to create a stronger password.

Recommendation 4 – Users should be required to use stronger passwords (a combination of letters/numbers/special characters) within My Account.

5.3.10 The Salesforce software was procured via the Government's G-Cloud framework contract. To be on the framework, the Software provider has had to satisfy central government that their product is both secure and compliant with data protection legislation.

5.3.11 Access to Salesforce is restricted to Council officers responsible for processing service requests (both within Customer Services and the specific service area). A review of current users found it to be up to date and suitable. It is advised that this is monitored on a regular basis (at least annually) to ensure access permissions remain up to date.

5.3.12 As at May 2016 Council Officers with access to personal information are required to have completed mandatory data protection e-learning in relation to their responsibilities for protecting personal information.

5.3.13 As at the start of July 2018, 29% of licensed users on Salesforce had not completed the training.

Recommendation 5 – Steps should be taken to ensure all Council Officers with access to sensitive personal information within Salesforce undertake the mandatory information governance e-learning, or have their access removed to the information.

5.3.14 The Council potentially shares some personal information within Salesforce with a third party. A suitable data sharing agreement is in place between the two organisations to ensure information is shared securely and confidentially.

5.3.15 Forms have been designed to ensure service users consent to their personal information being provided to the third party.

Appendix A – Management Action Plan

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Following project completion, measurements should be taken to determine if perceived benefits outlined at the project's onset have been realised.	M	Failure to identify and rectify failures to improve service delivery. Inability to apply lessons learned to future transition projects.	Ensure communications are in place between Customer Services and IT to measure the benefits outlined on the business case.	Customer Services Manager	Implemented
A process should be developed to archive and/or delete personal information held within both Salesforce and My Account, in line with suitable retention periods.	M	Council in possession of unnecessary personal information. Risk of breaching data protection legislation. Risk of fines and sanctions.	Scheduled deletion and disposal report tool is currently being configured. MyAccount specific privacy policy is being introduced with appropriate retention schedules applied.	Customer Services Manager	31 August 2018
A consent notice should be implemented within My Account that requires all registered users (both new and historic) to give consent to their personal information being used by the Council.	H	Risk of breaching data protection legislation. Risk of fines and sanctions.	Appropriate wording and hyperlink to the MyAccount privacy policy is under construction. Tick box will also be added to allow user to give explicit consent.	Customer Services Manager	31 August 2018

Appendix A – Management Action Plan

Summary of Recommendations and agreed actions					
Recommendations	**Priority**	**Risk Exposure**	**Agreed Action**	**Responsible Manager**	**Implementation Date**
Users should be required to use stronger passwords (a combination of letters/numbers/special characters) within My Account.	M	Personal data hacked from Council's application.	Investigating stronger password settings for MyAccount. If not possible, we will provide guidance on password strength.	Customer Services Manager	31 August 2018
Steps should be taken to ensure all Council Officers with access to sensitive personal information within Salesforce undertake the mandatory information governance e-learning, or have their access removed to the information.	M	Loss or breach of personal information due to officers failing to process in line with legislative requirement.	Email sent out 30/07/2018 to all advisors stating the need to complete the training. Management will monitor completion for each team member with the aim of all advisors compliant by 03/08/2018.	Customer Services Manager	3 August 2018

Appendix B

Audit Assurance Opinions

There are four levels of assurance used; these are defined as follows:

	Definition:	Rating Reason
Substantial	There is a sound system of internal control designed to achieve the system objectives and this minimises risk.	The control framework tested are suitable and complete are being consistently applied. Recommendations made relate to minor improvements or tightening of existing control frameworks.
Reasonable	There is a reasonable system of internal control in place which should ensure that system objectives are generally achieved, but some issues have been raised which may result in a degree of risk exposure beyond that which is considered acceptable.	Generally good systems of internal control are found to be in place but there are some areas where controls are not effectively applied and/or not sufficiently developed. Any high graded recommendations would only relate to a limited aspect of the control framework.
Partial	The system of internal control designed to achieve the system objectives is not sufficient. Some areas are satisfactory but there are an unacceptable number of weaknesses which have been identified and the level of non-compliance and / or weaknesses in the system of internal control puts the system objectives at risk.	There is an unsatisfactory level of internal control in place as controls are not being operated effectively and consistently; this is likely to be evidenced by a significant level of error being identified. High graded recommendations have been made that cover wide ranging aspects of the control environment.
Limited / None	Fundamental weaknesses have been identified in the system of internal control resulting in the control environment being unacceptably weak and this exposes the system objectives to an unacceptable level of risk.	Significant non-compliance with basic controls which leaves the system open to error and/or abuse. Control is generally weak/does not exist.

Appendix C

Grading of Audit Recommendations

Audit recommendations are graded in terms of their priority and risk exposure if the issue identified was to remain unaddressed. There are two levels of audit recommendations used; high and medium, the definitions of which are explained below.

	Definition:
High	Significant risk exposure identified arising from a fundamental weakness in the system of internal control
Medium	Some risk exposure identified from a weakness in the system of internal control

The implementation of agreed actions to Audit recommendations will be followed up at a later date (usually 6 months after the issue of the report).