IPSWICH
BOROUGH COUNCIL

SUFFOLK COASTAL DISTRICT COUNCIL Waveney District Council
in partnership

Internal Audit & Corporate Fraud Services

KEY ICT CONTROLS (AGRESSO) 2016-17

Report issued by:	Siobhan Martin - Head of Internal Audit
Report prepared by:	Paul Salmon
Date:	04/2017
Audit Reference:	RM030

DISTRIBUTION

Executive Portfolio Holder	
Audit & Governance Committee	
Chief Executive	R Williams
Chief Operating Officer	H Pluck
Head of Resource Management	D Field
Section 151 Officer	J Hudson
Assistant Operations Manager	B Burns
External Audit	T Meyer

FINAL

1.0 EXECUTIVE SUMMARY

1.1.1 Introduction

Internal Audit & Corporate Fraud Services acts in accordance with the Accounts and Audit Regulations (2015), Public Sector Internal Audit Standards and Local Government Application Note (2013). This audit has been prepared in accordance with our Audit Charter.

This audit is one of the reviews contained in the Audit Plan for the period 1st April 2016 to 31st March 2017 as approved by the Audit & Governance Committee on 01 March 2016. It involves a review of the access controls in operation over the Council's Financial system (Agresso).

This report sets out our findings and raises recommendations to address areas of weakness and/or non-compliance with existing controls, as set out in the action plan.

1.1.2 Audit Scope & Objectives

In planning this audit, a risk assessment has been undertaken, with the following considered to represent the potential key IT risks relating to the Council's Financial system (Agresso) which could impact on the Council's ability to deliver relevant Council Priorities and service objectives:

- Confidential data and information are accessed by unauthorised persons;
- Fraudulent or erroneous data is input and cannot be traced back to an individual person.

The objective of the audit was to ascertain the extent to which the identified risks have been managed and to evaluate whether effective controls to mitigate the risks have been established, and have been operating effectively throughout the period under review.

1.2 ASSURANCE STATEMENT

1.2.1 Overall Assurance Level**

Good	Adequate	Limited	Unsatisfactory
✓			

** For definitions see Appendix A

1.2.2 Positive Audit Comments

We would like to draw management attention to key controls in operation over Key ICT Controls (Agresso) 2016-17 processes and procedures that were operating effectively and efficiently:

- The password parameters comply with those stated in section 6.2 and Appendix A of the ICT Security Policy.
- All users have their own unique User ID, and all of the samples tested were

current employees.

- All roles assigned to users were appropriate based on their Organisational Unit/Job Role from HR4U.
- No user was both a 1st and 2nd level approver within the same Service Area.

1.2.3 Audit Report Follow-up

A follow-up review was undertaken to ensure that recommendations agreed in the previous audit report (Agresso Key Controls, RM020, April 2016) had been implemented. It was found that the one recommendation made has been implemented

1.2.4 Control Issues

This review has not identified any control areas where we consider that key improvements to current processes and procedures are needed or where there is the potential risk of fraud and corruption.

1.2.5 Adequacy of Individual Control Areas

Control Area	**Adequacy assessment ****	**Number of recommendations raised**		
		High**	**Medium****	**Low****
Key IT Controls - Agresso (Logical Access)	Good	0	0	1
Key IT Controls - Agresso (SoD)	Good	0	0	1
Total recommendations raised	2	0	0	2

** For definitions see Appendix A

1.3 ACKNOWLEDGEMENTS

We would like to thank management and staff for their co-operation during the course of this audit.

2.0 ACTION PLAN

1. Key IT Controls - Agresso (Logical Access)

REC No.	RISK	FINDING	RECOMMENDATION	REC. PRIORITY**	RESPONSIBLE OFFICER	MANAGEMENT IMPLEMENTATION DATE	MANAGEMENT RESPONSE
1	Data and information is accessed by unauthorised persons.	Based on a sample of 25 users, it would appear that over 25% of Agresso accounts have not been used for well over a year. Some of these users may have changed jobs, and the level of access may be inappropriate. Also, users who have not accessed Agresso for a long period are more prone to making errors.	Financial Services should obtain a report of all Agresso accounts that have not been used for over 1 year (with the assistance of ICT). They should run this report annually, and either contact the users to confirm they no longer need access to Agresso, and/or disable ('Park') the accounts.	Low	Team Leader - Management Accounting	31/07/2017	Agreed. User guidance notes are available on the intranet and any actions within the system (e.g. raising orders and paying invoices) are subject to further approval.

2. Segregation of Duties

2	Tasks are completed by unauthorised persons.	Although valid reasons were provided for the use of substitute users within Agresso, evidence of approval was not retained.	Requests for substitutions should be made by email from the user's line manager and should be retained by Financial Services as evidence.	Low	N/A	Complete	Agreed. This is related to ‘emergency’ substitutions. Email confirmation of any phone requests will be requested and retained.

** For definitions see Appendix A

APPENDIX A

3.0 OVERALL ASSURANCE LEVEL

Control Adequacy Assessments

We have four categories by which we classify our overall level of assurance of the processes examined and, also, the adequacy of the individual key control areas. They are defined as follows:

Good	All controls are being applied consistently and effectively. This means that all the control areas in the audit are being properly managed and the associated risks are being mitigated.
Adequate	Controls exist but there is some inconsistency in their application. This means that a few of the risks in the audit may need attention.
Limited	Some controls do not exist. This means that a reasonable number of the risks in the audit need attention.
Unsatisfactory	A significant number of controls do not exist and/or there are major omissions in the application of controls. This means that a significant number of risks in the audit are not being properly managed.

4.0 RECOMMENDATION PRIORITIES

We have three categories by which we classify our recommendations. They are defined as follows:

High	A top priority due to the absence of or non-compliance with a fundamental control process, creating the risk that significant error or malpractice could go undetected. These recommendations should normally be implemented within 1 to 3 months.
Medium	An important issue, which is needed to bring the internal control system up to an adequate standard or eliminate a serious level of non-compliance with an existing control process. These recommendations should normally be implemented within 1 to 6 months.
Low	An issue, which, if addressed, would contribute towards raising the standard of internal control to a level higher than adequate or help to reduce a less serious level of non-compliance with an existing control process. These recommendations should normally be implemented within 12 months.