AUDIT & RISK COMMITTEE

UPDATE ON AUDIT REPORTS GIVING LIMITED ASSURANCE

INTERNAL AUDIT REPORT

AGRESSO
2014-15

Issue Date:	3rd December 2014	*Issued to:*	Helen Briggs	Chief Executive
Author:	Trevor Croote		Debbie Mogg	Director of Resources
			Sav Della Rocca	Assistant Director - Resources
			Andrew Merry	Finance Manager
			Jason Haynes	Performance & Application Support Team Manager
			Councillor Edward Baines	Chairman of Audit & Risk Committee
			Councillor Terry King	Portfolio Holder (Finance)
			Councillor Martyn Pocock	Portfolio Holder (Resources)

AGRESSO 2014-15

EXECUTIVE SUMMARY

1. OVERALL OPINION

The Agresso system is a proprietary modular financial system. At Rutland it provides support for the main accounting system (general ledger), payroll, HR, debtors, creditors and cash receipting functions. The system operates by way of a layered 'workflow' which provides for separation of duties at key process stages. The effectiveness of the workflow depends on the establishment and maintenance of appropriate user profiles.

The key risks associated with the Agresso system were identified by officers as follows:
- user access rights may be inappropriate or out-of-date;
- inappropriate or uncontrolled super-user access; and
- system updates and patches are not properly tested or understood prior to going 'live'.

Officers asserted that any new or additional access to this system, beyond the minimum access rights, should be subject to formal approval by management to confirm that the access is appropriate and required for the job role. However, the audit found that arrangements for setting up, approving and maintaining user access rights were somewhat informal in practice and controls over super-user access were not fully effective.

Furthermore, it was identified that members of the Performance and Application Support (P&AS) team have the ability to access the system via any user's account without the knowledge or approval of the other user. This could enable the team members to make changes to the system that would be attributed to another council officer on the audit trail. Whilst controls over access rights could have been tighter, management asserted that there are compensating controls within systems that would highlight any wrongdoing e.g. if the P&AS team changed their salary levels, this would be picked up through the month end payroll review, budgetary control processes and HR checks. Controls over key financial systems are subject to separate audit reviews and to date Internal Audit has not identified any misuse of access rights.

Based upon the findings from the review, Internal Audit's opinion is that the design and operation of controls provides only **limited assurance** in respect of the identified risks. In coming to this conclusion it is acknowledged that immediate action was taken by management to resolve the key weaknesses as soon as they were identified by Internal Audit.

The audit was carried out in line with the scope set out in the approved Audit Planning Record. Appendices 1 and 2 summarise the controls identified and testing performed during the course of the audit.

The opinion is based upon testing of the design of controls to manage the three risks about which management sought assurance and testing to confirm the extent of compliance with those controls, as summarised in the table below.

Internal Audit Assurance Opinion	Direction of Travel
Limited Assurance	N/A

Risk	Design	Comply	Recommendations		
			H	**M**	**L**
Risk 1 – Inappropriate or out-of-date user access rights	**Sufficient Assurance**	**Limited Assurance**	1	0	0
Risk 2 – Inappropriate or uncontrolled 'super-user' access	**Limited Assurance**	**No Assurance**	3	0	0
Risk 3 – System updates and patches not properly tested or understood by users before going 'live	**Limited Assurance**	**N/A**	0	1	0
Other issues	**N/A**	**N/A**	0	2	0
Total Number of Recommendations			**4**	**3**	**0**

2. SUMMARY OF FINDINGS

Risk 1 – Inappropriate or out-of-date user access rights

Managers asserted that all new starters are only given minimum basic access rights and that any additional user privileges have to be approved by the employee's line manager. All changes to an individual's job/role are automatically notified to the P&AS team and relevant access privileges are revoked for certain high risk groups. Arrangements for modifying access privileges in respect of other lower risk staff are less formal and there are no arrangements for periodic review of access rights by managers.

Setting up of new users and changes to user access rights are fully logged within the system meaning that a complete audit trail is available.

For these reasons, the assurance rating for the design of controls is **sufficient assurance.**

Testing of a sample of new starters found that user accounts were set up in a timely manner in all cases. For three out of five cases tested there was no formal evidence of management approval of additional access privileges. Officers confirmed that arrangements for allocating additional access rights are largely informal and often based on discussions or emails from officers in the accountancy team rather than following a formal approval process.

For this reason, the assurance rating for compliance with control is **limited assurance**. Recommendation 1 addresses these issues.

Risk 2 – Inappropriate or uncontrolled 'super-user' access

There is currently one super-user role and four system administrator roles within the system. Officers were unable to provide precise details of the differences in functionality between each role, except to confirm that the super-user role is the most powerful as it provides uncontrolled access to all areas of the system and data.

Access to these roles is rightly limited to members of the P&AS team and the software supplier. In addition, officers asserted that access to the super-user role is only ever provided on a temporary basis following prior approval by the team manager, which is considered best practice. Whenever access is granted to the super-user role an automated alert is generated to inform the team manager. A further alert has recently been added to notify the team manager when access has been revoked.

At the time of audit there were two accounts that had been given permanent access to the super-user role since 29th May 2014 and were excluded from the alert system. These accounts were removed from the super-user role immediately after being brought to management's attention by the audit and all alert exclusions were also removed. During this period, controls could have been easily bypassed. However, for those activities that are logged within the system, testing confirmed that there is no evidence that one of these accounts was used during the relevant period. For the other account there is evidence that changes were made but, based on detailed analysis of data tables, management is satisfied that these were all legitimate changes.

During the audit it was noted that members of the P&AS team have the ability to log into the system under any existing user account without the knowledge or approval of the user. Officers asserted that this arrangement was established to improve the efficiency of dealing with technical support issues. Whilst this may be the most convenient arrangement for the P&AS team, it effectively provides them with the ability to undertake activities within the system that will be attributed to another user, which fundamentally undermines the audit trail. Again, management removed this functionality immediately following the issue being raised during the audit.

Furthermore, although user activity is logged for most functions, there is currently no simple way of extracting the audit trails, albeit there will always be a risk that super-users could delete or manipulate the audit trails.

For these reasons, the assurance rating for the design of controls is **limited assurance**.

Testing of all cases where temporary super-user access had been granted over the past 12 months found that formal evidence of prior management approval was available in only one out of nine occasions. There was evidence of the manager's awareness that access had been granted in one further case. Of the other occasions officers asserted that the manager of the P&AS team is located in the office with the team and requests were discussed in person but not formally documented.

For this reason, the assurance rating for compliance with controls is **limited assurance**. Recommendations 2, 3 and 4 address these issues.

Risk 3 – System updates and patches not properly tested or understood by users before going 'live'

Arrangements for managing updates, patches and system changes have been largely informal in the past but are in the process of being formalised. There are currently no documented procedures or a policy for change management, but the team has recently developed a formal change request form and change control form. At the time of audit, preparation of a formal change log was in progress and documentation for all changes is being retained on the network drive.

Given that the development of more formal arrangements remained work-in-progress at the time of audit, the assurance rating for the design of controls is **limited assurance**. Recommendation 5 addresses this issue.

The lack of formal procedures and absence of a completed change log meant it was not practical to undertake any compliance testing of system changes.

Other issues identified

As part of the review of controls related to user access rights it was noted that there are a total of 3,976 'roles' set up within the system, of which 1,830 (46%) are currently inactive. Furthermore, there are a number of examples of users that have been allocated roles that duplicate certain access rights. This creates a level of complexity that inevitably makes it more difficult for the P&AS team to maintain the system effectively and for managers to fully understand the precise functionality and access rights that have been allocated to themselves or their staff. Recommendation 6 addresses this issue.

It was also noted that a number of functions within the system are not currently logged (34 out of 88 data tables) and officers were unable to provide a clear explanation or justification for approximately 17 of these. This means that there is no audit trail for a number of activities and it is evident that system logging has not been subject to a recent review to ensure this remains appropriate. Due to lack of information available on the affected items there is uncertainty over whether this represents a significant risk. Recommendation 7 addresses this issue.

3. LIMITATIONS TO THE SCOPE OF THE AUDIT

The audit and associated testing was limited to the risks noted above and does not provide absolute assurance that material error, loss or fraud does not exist.

ACTION PLAN

Risk 1: Inappropriate or out-of-date user access rights						
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date
1	Arrangements for assigning or changing user access privileges for new starters and job changes are often informal and the requirement for manager approval is not enforced.	a) Any new users and changes to user access privileges should be made on an agreed form and signed off by the line manager and Finance Manager (to ensure non-finance staff are not given inappropriate access to finance only functions). b) Managers should be asked to periodically confirm user access rights.	Formal procedure agreed between Finance Manager and the P&AS team for part a). Part b) is under review to establish the best way to periodically review access rights to ensure they remain adequate.	High	P&AS Team Manager	**Nov 2014**

Risk 2: Inappropriate or uncontrolled 'super-user' access						
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date
2	Use of 'backup' accounts to provide the P&AS team with access in the event of inadvertent 'lock-outs' from their personal account could undermine the audit trail and bypass established controls.	P&AS Team Manager deletes the 'RCC Admin' and 'System' backup accounts and considers alternative means of dealing with inadvertent lock-outs by the P&AS team, if necessary.	Agreed. Already implemented	High	P&AS Team Manager	**Oct 2014**

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date
3	There is a lack of clarity regarding the functionality and therefore need for some of the existing administrator roles. In addition, whilst the Council complies with best practice by restricting access to these roles to a practical minimum, management of temporary access to the super-user role is not fully effective. Furthermore, extraction of audit trails is complicated and time consuming.	P&AS Team Manager improves controls over super-user and system admin accounts. In particular: a) seek clarification of the precise functionality and therefore need for each of the four administrator roles from the software supplier and delete any that are no longer required or unnecessary; b) ensure that prior management approval is given for all cases where SUPER access is granted and retain evidence of the approval; and c) work with the software supplier regarding the possibility of establishing a simple method of extracting audit trails and consider how this could be used to improve management and review of super-user activity.	Agreed. Administrator roles have been investigated and any out of date deleted. Use of super user role is being logged, but would like to point out that in most other Local Authorities the Super User role is given permanently to system administrators, so the restriction to the use already is greater than most of other LA's.	High	P&AS Team Manager	**Nov 2014**
4	The ability of the P&AS team to log in as any user fundamentally undermines system security and the effectiveness of audit trails.	Remove the ability of any member of staff, including the P&AS team, to log on to the system using another user's account. Develop controls to ensure that management are notified if any attempt is made to reinstate this functionality.	Agreed. Already removed	High	P&AS Team Manager	**Immediate**
Risk 3: System updates and patches not properly tested or understood by users before going 'live'						
5	Development of formal change management procedures remained a work in progress at the time of the audit.	Prepare a formal change management procedure including development and maintenance of a log of all change requests. The procedures should include a requirement to clearly establish responsibility for identification of training requirements at the outset.	Agreed. Completed, a formal change process is in place	Medium	P&AS Team Manager	**Nov 2014**

Other issues identified						
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date
6	There are a large number of unused roles and some users have roles that duplicate certain access rights. This creates unnecessary complexity that makes it more difficult to maintain the system effectively and for managers to fully understand the precise functionality and access rights allocated to themselves or their staff.	P&AS Team Manager reviews and rationalises the number of 'roles' within the Agresso system, in particular: a) consider deleting the 1,830 roles that are not currently used; and b) review roles allocated to staff with access to aggregated cost centres and remove individual cost-centre roles to avoid duplication where necessary.	Agreed. Current data cleanse process underway, looking at the whole agresso system not just roles. This will pick up both of the points raised.	Medium	P&AS Team Manager	**Dec 2014**
7	A number of functions within the system are not currently logged and officers were unable to provide a clear explanation for some of these. Without further details on the nature of the items affected, there is uncertainty over whether this represents a significant risk.	P&AS Team Manager seeks clarification from the software supplier of the detailed nature of all items not currently logged within the system and ensures that formal management approval is recorded in respect of any items where logging is to remain turned off.	Agreed. Investigation underway.	Medium	P&AS Team Manager	**Dec 2014**

INTERNAL AUDIT REPORT

COMMUNITY CARE FINANCE
(COURT OF PROTECTION & DEPUTYSHIP)
2014-15

COMMUNITY CARE FINANCE
(COURT OF PROTECTION & DEPUTYSHIP)
2014-15

EXECUTIVE SUMMARY

4. INTERNAL AUDIT OPINION

The Court of Protection has appointed the Council as a Deputy responsible for taking financial decisions on behalf of clients who are assessed, under the Mental Capacity Act, as unable to administer their own affairs and do not have family members willing or able to undertake those responsibilities on their behalf. The Council is currently the Deputy for five clients and there are two further potential clients pending. Overall, the Deputyship currently involves stewardship of assets totalling £470k.

The responsibility for the Deputyship role was transferred to the Revenues, Benefits and Community Care Team in 2012. It is important that the Council can demonstrate that the costs of care for clients have been correctly calculated, there has been proper stewardship of clients' assets; and that the Council has complied with statutory requirements. Whilst it could be seen that controls over the administration and management of clients' assets have been put into place, the execution of some key controls is inconsistent and would benefit from further development. Policies and procedures that govern the processes are also currently lacking. The portfolio of financial and residential assets is growing and the Council needs to ensure that controls are operating effectively and consistently in all cases.

Records are maintained by the Revenue, Benefits and Community Care team which itemise the transactions on each service user's account. However, review of the records highlighted that these require further development to ensure that sufficient detail is provided for all transactions and that supporting evidence (such as original invoices and till receipts) is retained for all expenditure. At the time of testing, evidence to support all expenditure was not readily available and the evidence that was held was not stored in a consistent and logical manner. Without supporting evidence in the form of invoices and till receipts, it is not possible to provide full assurance that the clients' monies have been appropriately spent and that all money from clients' bank accounts can be fully accounted for.   Regular independent checks and reconciliations of the records maintained by the team for the clients' finances should include confirming that suitable supporting evidence is retained, potentially on a sample basis.

For three of the five service users, the team issue money from the clients' accounts to carers and care homes to cover the costs of the service users' daily living needs. The carers are required to sign to confirm receipt of these payments to evidence the exchange of monies. In order to provide assurance over the legitimacy of the expenditure and identify any misuse of this money by the carers/care home staff, the Council should ensure that a detailed breakdown and supporting evidence is obtained to support all service user money provided. As a Deputy, the Council is responsible for safeguarding the clients' monies and ensuring all monies can be accounted for and are used for the intended purposes to benefit the service user. Each care home/carer who is given cash/cheques must maintain a record of all monies received and spent with supporting, original evidence for each item of expenditure which should be available for inspection by those charged with the Deputyship role. This should ensure all monies can be accounted for and act as a deterrent to any financial abuse.

Based upon the findings from the review, Internal Audit's opinion is that the current design and operation of controls provides **Limited Assurance** in respect of the identified risks.

The audit was carried out in line with the scope set out in the approved Audit Planning Record. Further information on the testing completed and detailed findings is available where requested. The opinion is based upon testing of the design of controls to manage the three risks about which management sought

assurance and testing to confirm the extent of compliance with those controls, as summarised in the following table:

Internal Audit Assurance Opinion		Direction of Travel		
Limited Assurance		**N/A**		
Risk	Design	Comply	Recommendations		
			H	**M**	**L**
Risk 1. The Council fails to demonstrate that it has calculated clients' costs of care correctly	Substantial Assurance	Sufficient Assurance	0	0	0
Risk 2. The Council fails to demonstrate proper stewardship of clients' assets	Limited Assurance	Limited Assurance	1	2	2
Risk 3. The Council fails to comply with statutory requirements relating to Deputyship	Substantial Assurance	Sufficient Assurance	0	0	0
Total Number of Recommendations			**1**	**2**	**2**

5. SUMMARY OF FINDINGS

Risk 1 The Council fails to demonstrate that it has calculated clients' costs of care correctly

Our review confirmed that there are policies in place to ensure that officers calculate clients' contributions correctly and the Council are able to demonstrate that they have done so. Furthermore, there is clear evidence that responsible officers have been proactive in pursuing clients' financial best interests by ensuring that all relevant benefits are claimed and by making best use of ISA allowances.

Arrangements are in place to engage with social workers to ensure that client action plans are developed in a transparent fashion.

No recommendations have been made in relation to this risk.

Risk 2 The Council fails to demonstrate proper stewardship of clients' assets

Currently, formal policies and procedures do not exist for the management and administration of client finances which has led to inconsistencies in how supporting documentation for each client has been retained. ***Recommendation 1 addresses this issue.***

A sample of five expenditure transactions per client (25 in total) were selected for review during the audit to ensure that there was appropriate supporting documentation and each transaction could be accounted for. Testing proved difficult initially as filing of documents to support the clients' finances was generally illogical and inconsistent.

- 23 out of 25 transactions could be fully accounted for;
- The two remaining transactions included a payment to a care home of £3,000 for which evidence of payment could not be provided at the time of testing but the care home has verbally confirmed receipt of the monies; and
- Evidence could not be provided for a further payment, which related to a service user who has access to a cheque book and debit card. It is understood that the service user incurred this expenditure. This arrangement is in place following a court ruling that the Deputyship arrangement for this individual should support independence. On this account, the team do not have access to any debit cards and the cheque numbers distinguish between those held by the team and those

held by the client. The Deputyship team should log any transactions undertaken by the service user to ensure that the team are protected from any allegations of theft or fraud.

- Five of the sample of payments related to cheque or cash given to care homes/carers for personal expenses of the clients. Two signatories are required for all cheque payments and there is a receipting system in place for cash payments. However, care homes do not consistently provide an itemisation of how the money was spent and they are not required to provide invoices/receipts to support each payment. Accountability for the management of these clients' finance lies with the Council and, therefore, the Council should be provided with assurance that the monies are being spent on the intended goods/services for the client.
  Recommendations 2, 3 and 4 address these issues.

Risk 3 The Council fails to comply with statutory requirements relating to Deputyship

The Council is required to comply with Section 1 of the Mental Health Act 2005 and to have regard to the Code of Conduct to the Act.

The Constitution of the Council clearly allocates responsibility for Court of Protection issues to the Director for People and there is an established protocol to evidence allocation of responsibility for financial administration to the Revenues and Benefit Manager and the Benefits Team Leader.

Responsibility for financial administration is vested in appropriately senior and relevantly experienced Officers and separation of duties between the Revenues and Benefit Team (financial administration) and social workers (assessment of care needs) addresses the issue of potential conflicts of interest.

The Council must submit annual, mandatory Deputy Declaration reports to the Office of the Public Guardian (OPG) to account for all decisions made by the Deputy on behalf of the client. Testing confirmed that these declarations had been submitted accordingly. It was identified, however, that there are currently no internal reporting mechanisms whereby those charged with Deputyship responsibilities must account for financial decisions made on behalf of clients to senior management during the year and the formal declaration forms submitted by the team to the OPG are not subject to independent, internal review before submission. As such, it is recommended that an internal reporting procedure be implemented whereby the financial decisions are subject to review by a senior manager on a regular basis to confirm these are appropriate and in the interests of clients. The reports could be based upon the form submitted to the OPG and should demonstrate the decisions made and the impact on the clients' finances. This review process should culminate in the senior manager reviewing and agreeing the annual deputyship declaration reports before submission. *Recommendation 5 addresses this issue.*

3   LIMITATIONS TO THE SCOPE OF THE AUDIT

The Auditor's work does not provide any guarantee against material errors, loss or fraud. It does not provide absolute assurance that material error; loss or fraud does not exist.

ACTION PLAN

No.	ISSUE	RECOMMENDATION It is recommended that ...	Management Comments	Category	Officer Responsible	Due date	WP Ref
Risk 2 : The Council fails to demonstrate proper stewardship of clients' assets							
1	Currently, formal policies and procedures do not exist for the management and administration of client finances which has led to inconsistencies in how supporting documentation for each client has been retained.	Revenues and Benefits Manager to develop policies and procedures relating to the day to day administration and management of client finances. These are to be formally approved and disseminated to appropriate staff.	Agreed. End of January	M	Revenues and Benefits Manager	End January 2015	02.01.01
2	Evidence should be retained to support all expenditure from service users' accounts to demonstrate that all transactions are genuine and that all monies can be accounted for.	A standard electronic indexing system to be developed by the Revenues and Benefits Manager to enable the retention and retrieval of clients' financial documentation. Each client file should, as a minimum requirement, hold the following documentation: - Scanned copies of all bank statements; - A cash book, recording all income and expenditure; and - Scanned receipts and/or invoices supporting all transactions from the client's bank account. Regular sample checks and reviews of the accounts, including checks that supporting evidence is provided to	Agreed, end November. AD (Finance) will undertake a quarterly inspection of accounts.	H	Revenues and Benefits Manager	End November 2014	02.01.01

5

Risk 2 : The Council fails to demonstrate proper stewardship of clients' assets							
No.	ISSUE	RECOMMENDATION It is recommended that ...	Management Comments	Category	Officer Responsible	Due date	WP Ref
		account for all transactions should be conducted and recorded by an independent Senior Manager.					
3	For three of the five service users, the team issue money from the clients' accounts to carers and care homes to cover the costs of the service users' daily living needs. The carers are required to sign to confirm receipt of these payments. However, in order to provide assurance over the legitimacy of the expenditure and identify any misuse of this money by the carers/care home staff, the Revenue and Benefits team should ensure that a detailed breakdown and supporting evidence is obtained to support all service user money received. Furthermore, the requirement to detail and evidence all expenditure and make this available for review should also act as a deterrent to any potential financial abuse.	The Revenues and Benefits Manager ensures that carers are required to provide a full itemisation of the use of the cheque/cash payments for clients' daily costs, along with receipts to fully support this. These records should be reviewed by the Deputyship team on a regular basis. The frequency of these checks should be formally agreed and documented within the Council's policies on management of client finances. Checks should be made to ensure: • Total monies received reconcile to records maintained by the team of total monies provided; • Expenditure is full supported by invoices/receipts; • Expenditure on receipts appears reasonable and appropriate; • Running balances are arithmetically correct; and • Where relevant, each service	The Council will require all those receiving monies on behalf of others to sign an appropriate declaration. It will also undertake a sample check of how funds are being used.	H	Revenues and Benefits Manager	End November 2014	02.01. 01

Risk 2 : The Council fails to demonstrate proper stewardship of clients' assets							
No.	ISSUE	RECOMMENDATION It is recommended that ...	Management Comments	Category	Officer Responsible	Due date	WP Ref
		user's monies are held and accounted for separately i.e. not consolidated with other care home residents' accounts. Agreements with care homes should include 'open book' access to records of client finances, where possible.					
4	Deputyship arrangements can vary depending upon the assessed ability of the client. A court ruling for one of the clients supported by the Council stated that their arrangement should be unobtrusive and enable independence. As such, this client has access to a debit card and cheque book. This arrangement introduces further risk, as there are payments on the client's bank statement that the team cannot provide evidence to support. The team should not have access to any debit cards and the cheque numbers should distinguish between those held by the team and those held by the client. The Deputyship team should review how the expenditure is recorded and accounted for in relation to this account to ensure that the	When reviewing the evidence held to support payments on this account (see recommendation 2), the reviewer should confirm that those which are not suitably supported and accounted for relate to either debit card payments or cheque numbers from the client's book only.	The team will keep evidence of cheque books issued and note which transactions have been made by the user directly.	M	Revenues and Benefits Manager	End November 2014	02.01.01

No.	ISSUE	RECOMMENDATION It is recommended that ...	Management Comments	Category	Officer Responsible	Due date	WP Ref
Risk 2 : The Council fails to demonstrate proper stewardship of clients' assets							
	team are protected from any allegations of theft or fraud.						
5	At present there is no formal requirement for the Revenues & Benefits team to account internally for their performance as they discharge the Deputy role and act as stewards for clients' assets and interests. The mandatory Declaration forms are also not subject to review before submission to the OPG.	The Revenues & Benefits Manager submits periodic reports to the Director for People which account for financial decisions taken on behalf of clients; these reports could be based upon the template for relevant sections of the formal Deputy's Declaration form. The annual Deputy's Declaration to the OPG should also be reviewed and agreed as accurate by a senior manager before submission.	Agreed	L	Revenues and Benefits Manager	31 March 2015	02.01.01