Paper A2

Item 6

Final Report

SWAP
SOUTH WEST AUDIT PARTNERSHIP
Delivering Audit Excellence

Somerset County Council

- Adults Integrated Solution (AIS) 2012-13 report

Issued to: Alan Webb
Head of ICT

Helen Wakeling
Adults and Health
Operations Director

Barrie Fitzpatrick
Adult Social Care Operational
Commissioning Manager

Mark O'Brien
Southwest One
Chief Information Officer

Kevin Nacey
Head of Property & Finance

Martin Gerrish
Group Manager, Advisory Finance

Gerry Cox
Chief Executive SWAP

Adults Integrated Solution (AIS)

Management Summary

Northgate's Adults Integrated Solution (AIS) is the application used by Adult Social Care (ASC) to support the adult care management processes. Northgate designed the application to support the personalization agenda and it offers practitioners a web-based interface and a fully integrated environment to enable them to deliver personalized support planning, care brokerage and commissioning.

A search for a solution to replace SWIFT was initiated due to the excessive cost of maintaining Version 21. The SAP ASC module was evaluated and was found to be unacceptable. As a result In April 2011 the SWIFT application was upgraded to AIS/SWIFT Version 25. SWAP postponed a review of AIS at that time due to serious performance problems. In spite of continued discussions between Southwest One and Northgate and related infrastructure modifications, performance issues persist. The current release is Version 27.02.

Due to the size and complexity of the AIS application, the scope of this review was limited. SWAP did not perform a detailed review of the use of spreadsheets and the Direct Payments process since these are being addressed in other SWAP audits. However information gained in this audit was shared with the other SWAP auditors.

Summary of Significant Corporate Risks

The following table records the inherent risk (the risk of exposure with no controls in place) and the manager's initial assessment of the risk (the risk exposure on the assumption that the current controls are operating effectively) captured at the outset of the audit. The final column of the table is the Auditors summary assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Areas identified as significant corporate risks, i.e. those being assessed as 'high' or 'very high' risk areas in line with the definitions attached should be addressed as a matter of urgency.

Risks	Inherent Risk Assessment	Managers Initial Assessment	Auditors Assessment
Application does not meet business and Data Protection requirements	Medium	Medium	High
Unauthorised access and disclosure of sensitive information	Medium	Medium	Medium

Application availability cannot be assured	Medium	Medium	High

Summary of Significant Findings

- Responsibilities related to AIS have not been formally documented including the naming of a system owner.
- There are no reports or processes, other than database monitoring that ensure the ongoing integrity of AIS data and the appropriateness of payments.
- If the SCC Data Centre was unavailable for any reason, applications could be unavailable for a month or even more.
- Since the implementation of AIS two years ago, performance and response time have been a major issue that has not been resolved to the satisfaction of ASC Operations.

Further details of audit's findings can be viewed in the full audit report, which follows this Management Summary.

Conclusion and Audit Opinion

Partial

I am able to offer Partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Formalised roles and responsibilities have not been developed for the entities involved with the management and operation of AIS. These include ASC Operations, SCC Finance, the AIS Programme Board chaired by Barrie Fitzpatrick, Southwest One, ICT and Northgate. Also there is no formally named business system owner.

There are no reports or processes, other than database monitoring, to ensure the ongoing integrity of AIS data, for example by comparing a report of key values from the AIS database at different points in time for appropriateness. This would be of particular value when a new release or a system change is implemented to ensure no data has been lost and corrupted. In addition there does not appear to be a process to ensure payments are authorised, appropriate, complete and accurate.

We have identified in previous audit reports that there is no tested IT Disaster Recovery strategy. This is a strategy that would be put into effect in the event the SCC Data Centre was unavailable for any reason. Although a contract has been signed with Adam Continuity, applications could still be unavailable for a month or even more.

AIS performance and response time issues persist two years after implementation. There is no

contractual requirement or SLA for Southwest One to provide a platform that delivers performance and response time that is acceptable to ASC Operations. We also noted that there is no volume testing strategy that would identify any degradation of performance in advance of the implementation of an upgrade or major change.

Data quality in AIS data is undermined by the lack of robust input validation within the AIS application. Client records can be created with a minimum of information. Key personal identifiers such as data of birth, NI number and NHS number do not need to be entered and this both increases the risk of duplicate records and provides less data with which to identify those that have been created. Validation reports are produced to identify missing data and facilitate collecting missing information.

The database team in Southwest One ensure the structural and referential integrity of the database but there are no reports to facilitate review or monitoring the integrity of AIS data by users. We recognise it is not possible to provide control total reconciliations for a real time online system but overall activity and key transactions or events, such as the level of care packages under the £1000 approval de minimis, payments on behalf of clients where a date of death is recorded, could be reported for review.

AIS information is processed in other systems, notably the Protocol children's care database and SAP financial system. The interface with Protocol can create duplicate records and records removed or archived from AIS are not automatically removed from Protocol thereby leaving the systems out of sync and causing a potential retention of data issue under the Data Protection Act.

We were unable to assess the controls over the interface between AIS/SWIFT and payments to care providers (direct payments are the subject of a separate audit) generated in SAP. However we note that the payments process is heavily dependent on Excel workbooks and SAP GL codes are not directly used but are applied via a lookup from the previous CedAR financial system codes. Independent Service Provider (ISP) functionality in AIS is being considered for supplier billing and may be able to replace some of the spread sheet processes.

The full benefit of AIS automation is not being derived in other areas of operation, for example Case allocation is dependent on Excel workbooks although there are plans to implement AIS allocation.

Implementation of access control in AIS lacks granularity and it is possible some users have more access than they require. Apart from the vendor support accounts any disclosure arising from this would be to users in the adult social care workforce. We were unable to determine if AIS audit trail and logging processes capture sufficient information to trace activity in the system.

Southwest One currently owns the contract with Northgate and would not provide SWAP with a copy. As a result SWAP was not able to evaluate Northgate's compliance with the terms of the contract including licensing requirements. In addition information was not provided to evaluate controls over the interfaces between AIS/SWIFT, intermediary systems and SAP and to evaluate the adequacy of audit trails and logs.

Several issues were raised in recent SWAP audits that have bearing on the AIS application and although already reported, they are repeated here due to their significance. It was noted that developers have access to the production environment, unmasked live production data is used by developers and vendors for testing purposes and desktops are not locked down.

The majority of the concerns raised above apply to all one hundred and twenty applications supported by Southwest One for Somerset County Council, of which sixteen, including AIS, are classified as critical. SWAP was informed SAP is an exception since developers do not have access to the production environment and production data is masked during testing.

Detailed Audit Report

Objectives & Risks

The key objective of the service and risks that could impact on the achievement of this objective were discussed and are identified below.

Objective: To ensure that the AIS application operates securely with maximum system availability to provide accurate, timely and compliant data and management information, as a key enabler for effective service delivery.

Risks:

- Application does not meet business and regulatory requirements
- Unauthorised access and disclosure of sensitive information
- Application availability cannot be assured

Method & Scope

This audit has been undertaken using an agreed risk based audit. This means that:

- the objectives and risks are discussed and agreed with management at the outset of the audit;
- the controls established to manage risks are discussed with key staff and relevant documentation reviewed;
- these controls are evaluated to assess whether they are proportionate to the risks and evidence sought to confirm controls are operating effectively;
- at the end of the audit, findings are discussed at a close-out meeting with the main contact and suggestions for improvement are agreed.

AIS is the care management application and database used by Adult Social Care. The audit considers:

- Controls that ensure the relevance and reliability of the information provided by the application and that exchanged/interfaced with linked systems. This will include data entry and validation checks, data integrity checks, the extent of management information and performance reports, user training and how the application can be used to ensure compliance with the regulatory obligations of the service.

- Control of vendor and ICT changes to the application and changes to parameter data that impact on application processing and operation.

- The access policy and controls that regulate and monitor access (including third parties and vendor support) to the application and data.

- Vendor and ICT support and maintenance arrangements.

- Arrangements to recover the application in the event of a major outage.

Findings

The following paragraphs detail all findings that warrant the attention of management.

The findings are all grouped under the objective and risk that they relate.

1. Risk: Application does not meet business and regulatory requirements

1.1 There are several entities involved with the management and operation of AIS including ASC Operations, SCC Finance, the ICT client, Southwest One, Northgate, and the AIS Programme Board chaired by Barrie Fitzpatrick. There is no formally named business system owner who is the focal point for decisions relating to the application. Without formalised roles and responsibilities an appropriate level of communication and governance may not exist. SWAP was advised individual owners have not been assigned for the majority of the SCC applications.

1.1a It was agreed that the roles and responsibilities of ASC Operations, SCC Finance, Southwest One, ICT, the AIS Programme Board and the AIS System owner be clearly defined to ensure effective communications and decision making. Helen Wakeling, the Caldicott guardian, has been fulfilling the role of AIS System Owner which needs to be formalised.

1.2 The quality of AIS data is undermined by the lack of robust input validation included in the AIS application. The application allows a record to be created with only the client name and address although many more fields are required, e.g. date of birth, sex and ethnicity. There is no process in place for authenticating the client, for example by verifying against their National Insurance (NI) number or NHS number. The use of the client name as the key creates the potential for duplicate client records being created since clients may have aliases. Although Information Management produces validation reports of records added to AIS that are missing data elements, identifying and correcting data after it has been added to AIS is inefficient and not cost-effective.

1.2a It was agreed that the AIS System Owner should require that AIS is modified to include robust validation and authentication, and should consider using an unique identifier, such as NHS or NI number, as the key. Information Management should identify potential duplicates for analysis and review by ASC Operations.

1.3 The interface between AIS & Protocol, which adds or modifies demographic data to keep the databases in sync, can create a duplicate record in both AIS and Protocol. Also when a record is deleted from AIS, as required after 7 years of no case contact, there is no automated process to remove the record from Protocol, creating a potential Data Protection issue. Swap was advised a project is underway to address the deletion of records. In addition although it was not possible to assess the controls over AIS/SWIFT and SAP interfaces, it was noted that the SAP General Ledger codes have not yet been introduced.

1.3a It was agreed that the AIS and Protocol System Owners should consider a more appropriate and robust solution for the sharing of data between the AIS and Protocol applications.

1.3b It was agreed that controls that ensure the completeness, accuracy and security of AIS/SWIFT and SAP interfaces should be documented by Southwest One and made available for review by the AIS System Owner and SWAP. AIS/SWIFT should be modified to utilise SAP general ledger codes.

1.4 There is no document that describes decisions and the rationale for utilising certain AIS functionality and for not using other functionality. In addition the Digital Dashboard, designed to provide critical performance data, has still not been delivered. Allocation and Independent Service Provider (ISP) billing functions available in AIS, are performed using spreadsheets that could be insecure, may be exposed to inappropriate view and update by non-ASC users and may not be backed-up. Finance uses spreadsheets and manually compares supplier bills to AIS data rather than sending out bills using the ISP billing functionality. AIS automation is not always being used to full advantage and the use of spreadsheets as an alternative may be insecure and prone to error.

1.4a It was agreed that the AIS System Owner document decisions and rationale for which AIS functionality is and is not being utilised in AIS and expedite the implementation of the Digital Dashboard.

1.4b It was agreed that the AIS System Owner obtain from Southwest One details of the security and back-up procedures over all spreadsheets used by ASC Operations and SCC Finance. This should be evaluated and recommendations for enhancements made where required.

1.5 There are no reports or processes, other than database monitoring, to ensure the ongoing integrity of AIS data, for example by comparing a report of key values from the AIS database at different points in time for appropriateness. This would be of particular value when a new release or a system change is implemented to ensure no data has been lost and corrupted. In addition there are no reports that are reviewed by ASC Operations that ensure the appropriateness of payment transactions. With no direct interface between AIS and SAP from which payments are made, without a common identifier, and without the recording of payments in AIS, there does not appear to be a process to ensure payments are authorised, appropriate, complete and accurate. In addition the authorise function, a security feature available in AIS has not been implemented resulting in all authorisations occurring outside of AIS. As a result data loss, potential corruption of data, incorrect and potentially fraudulent use of the application, missed, inappropriate or additional payments, will not be identified and acted upon.

1.5a It was agreed that the AIS System Owner require the implementation of reporting and related review processes to monitor and ensure the ongoing integrity and the appropriateness of AIS data and related payment transactions. Possible examples include reporting daily totals of critical values (such as total clients, total approved care package), excessive orders for services below the £1,000 approval threshold, payments in excess of the approved care plan, payments after date of death applied, reversal of date of death, and an automated comparison of payments made from SAP to AIS for appropriateness.

2. Risk: Unauthorised access and disclosure of sensitive information

2.1 Our review of AIS security showed that:

- Security implemented is not granular in nature providing many of the 775 users with more access than they need to perform their job functions.
- Five super users in Southwest One have security administrator capability, unlimited and unmonitored update access to AIS. Several generic user ids, established by Northgate and whose purpose is unclear, are made available to these super users, with the password distributed via email.
- Passwords are reset by the Help Desk who provide a password that is not a one-time password. Approximately 25% of users reset their passwords in the one month prior to our meetings.
- In spite of a recent security incident that appeared to result in some data corruption, there is no reporting in place or review of user, super user or generic user access for appropriateness.
- Terminated users were identified with valid AIS access credentials. Just less than 10% of managers with access were found to be no longer employed. In addition user ids are not disabled after not being used for a period of time.
- The time-out for the application is 1 hour. Although users typically leave the application on and lock the screen when they go out to lunch, this process is inefficient, leaving sessions unavailable for others and insecure, since the user could forget to lock their screen and allow bypass of all security.

The lack of granular security, absence of reporting and monitoring, absence of robust leavers and password reset procedures all contribute to the potential for unauthorised access and update to AIS data that would not be identified. SCC has a duty of care in this respect to ensure personal data is not used inappropriately.

2.1a It was agreed that the AIS System Owner discuss the AIS security capabilities with Northgate and develop their AIS access requirements which ensure the appropriate segregation of duties and duty of care over personal data. Additional actions required include but are not limited to implementing an annual manager review and approval of current access, monitoring user and super user access, eliminating the use of generic user ids, locking user ids that have not be utilised in a specific period of time and implementing a robust leavers process and password reset procedure.

2.2 Although SWAP noted that AIS does not maintain the user id of the person who added a client record, we were unable to obtain details regarding the configuration of audit trail and logs. Hence we are unable to determine if the audit trail and logs provide sufficient information to trace and attribute activity in the system.

2.2a It was agreed that options exercised over the audit trail and logs currently maintained in AIS should be documented by Southwest One AIS Security Administrator in order that the AIS System Owner can assess its adequacy for routine and potential fraud related investigations

2.3 We identified during our audit of the Systems Development Life Cycle that unmasked AIS data is used in the development environment by developers and vendors. SWAP recommended a risk assessment be performed and data should be masked or other mitigating controls introduced. We also identified in our Capacity Management audit that desktop lockdown is not in effect and as a result AIS data can be downloaded and copied to USB flash storage. SWAP recommended data security policies be developed and implemented.

3. Risk: Application availability cannot be assured

3.1 We have identified in previous audit reports that there is no tested IT Disaster Recovery strategy. This is a strategy that would be put into effect in the event the SCC Data Centre was unavailable for any reason. Although a contract has been signed with Adam Continuity, applications could still be unavailable for a month or even more. The ASC emergency plan relies on to tracking activity using pink sheets, a process that may not be robust enough for that period of time.

3.1a It was agreed that the AIS system owner review the current emergency plan to ensure it is adequate for an outage of one month or more. In addition the AIS System Owner should ensure the plans address the continuation of payments and addresses the need for on-going client communications.

3.2 The AIS vendor support contract has been novated to Southwest One who were unwilling to share the contract details with SWAP. We are therefore unable to determine whether the contract adequately addresses performance, guarantees and penalties. This is of concern since performance and availability has been an issue since AIS/SWIFT was implemented.

3.3 Although it was not possible to determine the adequacy of patch management, and whether it complies with the contractual arrangements, we noted that issues identified in new release testing are not always addressed by Northgate resulting in workarounds having to be implemented by AIS users. In addition Northgate do not track and share with ASC the remaining unresolved issues. As a result new releases are not implemented with all identified problems resolved and the full benefits of automation are not being derived as workarounds are added.

3.3a It was agreed that the AIS System Owner should require that issues are tracked to completion. If they cannot be implemented in the current release they should be tracked, reported and added to the next release or patch. The contract should be reviewed to determine if there are ramifications of not fixing known documented problems.

3.4 Since information relating to licensing of AIS has been withheld by Southwest One, it is impossible to determine if the number of AIS and supporting software licenses is being monitored for appropriateness and complies with licensing regulations. Although non-compliance with licensing laws is now the responsibility of Southwest One, if a problem were to arise SCC could be negatively impacted.

3.5 Since the implementation of AIS two years ago, performance and response time have been a major issue that has not been resolved to the satisfaction of ASC. Inadequate response time impacts the productivity of the 775 AIS users. In addition it was recently reported in the Capacity Planning Audit Report that there is only one overall SLA between Southwest One and SCC which is not specific to AIS and does not address response time. We also noted that there is no testing strategy that would identify any degradation of performance in advance of the implementation of an upgrade or major change.

3.5a **It was agreed that the AIS System Owner require the implementation of an SLA which addresses an acceptable response time e.g. 2 – 5 seconds. In addition I recommend the AIS System Owner, Head of ICT and Southwest One consider and determine the feasibility of implementing a robust testing environment which is not contractually required.**

The Agreed Action Plan provides a formal record of points arising from this audit and, where appropriate, the action management has agreed to take and the timescale in which the action will be completed. All findings have been given a priority rating between 1 and 5, where 1 is low and 5 is high.

It is these findings that have formed the opinion of the service's control environment that has been reported in the Management Summary.

Adults Integrated Solution (AIS)

Confidential **Agreed Action Plan**

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
Objective: **To ensure that the AIS application operates securely with maximum system availability to provide accurate, timely and compliant data and management information, as a key enabler for effective service delivery.**					
1. Application does not meet business and regulatory requirements					
1.1a Responsibilities related to AIS have not been formally documented including the naming of a system owner.	I recommend that the roles and responsibilities of ASC Operations, SCC Finance, Southwest One, ICT, the AIS Programme Board and the AIS System owner be clearly defined to ensure effective communications and decision making. Helen Wakeling, the Caldicott guardian, has been fulfilling the role of AIS System Owner which needs to be formalised. *SWAP Ref: 21842*	4	Roles and responsibilities will be discussed at the the AIS Programme Board. They will be documented and will include system ownership and the responsibility for signoffs required by ASC and SCC Finance.	AIS Programme Board, Barrie Fitzpatrick, Helen Wakeling, SCC Finance	31 December 2013
1.2a AIS data quality is undermined by the lack of robust input validation.	I recommend that the AIS System Owner should require that AIS is modified to include robust validation and authentication, and should consider using an unique identifier, such as NHS or NI	3	ASC needs the flexibility to be able to enter minimum data to ensure timely care is provided. However there is a project to validate the NHS #, if entered in AIS. A report will be requested	AIS System Owner, Information Management	31 December 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	number, as the key. Information Management should identify potential duplicates for analysis and review by ASC Operations. *SWAP Ref: 21305*		from Information Management to identify potential duplicates for investigation and action.		
1.3a The interface between the AIS and Protocol applications can create duplicates.	I recommend the AIS and Protocol System Owners should consider a more appropriate and robust solution for the sharing of data between the AIS and Protocol applications. *SWAP Ref: 21242*	3	A PIR will be submitted proposing a joint review of the process with consideration for sharing rather than propagating data	AIS System Owner	31 December 2013
1.3b Interface controls between AIS & SWIFT could not be assessed.	I recommend that controls that ensure the completeness, accuracy and security of AIS/SWIFT and SAP interfaces should be documented by Southwest One and made available for review by the AIS System Owner and SWAP. AIS/SWIFT should be modified to utilise SAP general ledger codes. *SWAP Ref: 23455*	3	AIS System owner will request that Southwest One document the controls that ensure the completeness, accuracy and security of AIS/SWIFT and SAP interfaces. Consideration will be give to the use of SAP general ledger codes in the project considering using Block Contracts, ISP and Direct payment functionality in AIS/Swift.	AIS System Owner	31 December 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
1.4a The rationale for utilising certain AIS functionality and for not using other functionality has not been documented.	I recommend the AIS System Owner document decisions and rationale for which AIS functionality is and is not being utilised in AIS and expedite the implementation of the Digital Dashboard. *SWAP Ref: 21247*	3	At a meeting of the AIS Programme Board a project will be initiated to document decisions and rationale for which AIS functionality is and is not being utilised in AIS. The issues related to the implementation of the Digital Dashboard have already been raised with senior management and are being addressed.	AIS System Owner	31 December 2013
1.4b Functions available in AIS are being performed in spreadsheets that may not be secure.	I recommend that the AIS System Owner obtain from Southwest One details of the security and back-up procedures over all spreadsheets used by ASC Operations and SCC Finance. This should be evaluated and recommendations for enhancements made where required. *SWAP Ref: 23449*	3	AIS System owner will request this information from Southwest One, evaluate and take appropriate action.	AIS System Owner	31 December 2013
1.5a. There are no reports or processes, other than database monitoring that ensure the	I recommend the AIS System Owner require the implementation of reporting	4	AIS System owner will develop reporting requirements.	AIS System Owner	31 December 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
ongoing integrity of AIS data and the appropriateness of payments.	and related review processes to monitor and ensure the ongoing integrity of AIS data and the appropriateness of related payment transactions. Possible examples include reporting daily totals of critical values (such as total clients, total approved care package), excessive orders for services below the £1,000 approval threshold, payments in excess of the approved care plan, payments after date of death applied, reversal of date of death, and an automated comparison of payments made from SAP to AIS for appropriateness. *SWAP Ref: 21311*				
2. Unauthorised access and disclosure of sensitive information					
2.1a AIS security provides the potential for unauthorised access and update to AIS data.	I recommend that the AIS System Owner discuss the AIS security capabilities with Northgate and develop their AIS access requirements which ensure the appropriate segregation of duties and duty	3	AIS System owner will request Security documentation from Northgate, evaluate current security and develop access requirements	AIS System Owner Northgate	31 December 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	of care over personal data. Additional actions required include but are not limited to implementing an annual manager review and approval of current access, monitoring user and super user access, eliminating the use of generic user ids, locking user ids that have not be utilised in a specific period of time and implementing a robust leavers process and password reset procedure. *SWAP Ref: 21244*				
2.2a The AIS audit trail does not provide details of the last user access.	I recommend that options exercised over the audit trail and logs currently maintained in AIS should be documented by Southwest One in order that the AIS System Owner can assess its adequacy for routine and potential fraud related investigations. *SWAP Ref: 21251*	3	ASC Response We will request this information from Southwest One, evaluate and take appropriate action when it is provided. Southwest One Response: SWOne maintains controls at the server and database levels. If the AIS System Owner has specific controls requirements for the application, SWOne is willing to work with Northgate	Southwest One AIS System Owner	31 December 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
			and the AIS System Owner to determine a solution.		
3. Application availability cannot be assured					
3.1a If the SCC Data Centre was unavailable for any reason applications could be unavailable for a month or even more.	I recommend that the AIS System Owner review the current emergency plan to ensure it is adequate for an outage of one month or more. In addition the AIS System Owner should ensure the plans address the continuation of payments and addresses the need for on-going client communications. *SWAP Ref: 21243*	4	We will review the current plan to determine what changes are will be necessary for an outage of a month or more. We will meet with Corporate Business Continuity Planning to ensure all plan address possible contingencies.	AIS System Owner	31 December 2013
3.4a Issues identified in new releases are not always addressed by Northgate	I recommend the AIS System Owner should require that issues are tracked to completion. If they cannot be implemented in the current release they should be tracked, reported and added to the next release or patch. The contract should be reviewed to ensure all	3	We will implement a formal process with Northgate to track issues identified in testing through to completion. This will include detailed analysis of all service packs and releases to further track what changes and fixes are being implemented.	AIS System Owner	30 November 2013

Finding	Recommendation	Priority Rating	Management Response	Responsible Officer	Implementation Date
	available penalties are claimed for not fixing known documented problems. *SWAP Ref: 21250*				
3.5a Performance and response time of AIS has been a major issue since the implementation of AIS two years ago and has not been resolved to the satisfaction of ASC Operations.	I recommend that the AIS System Owner require the implementation of an SLA which addresses an acceptable response time e.g. 2 – 5 seconds. In addition I recommend the AIS System Owner, Head of ICT and Southwest One consider and determine the feasibility of implementing a robust testing environment which is not currently contractually required. *SWAP Ref: 22000*	4	We will meet with Southwest One to discuss the development of an SLA and the feasibility of a implementing a robust testing environment.	AIS System Owner Head of ICT	31 December 2013

Audit Framework Definitions

Control Assurance Definitions

Substantial		I am able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.
Reasonable		I am able to offer reasonable assurance as most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial		I am able to offer Partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
None		I am not able to offer any assurance. The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Categorisation Of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors, however, the definitions imply the importance.

Priority 5: Findings that are fundamental to the integrity of the unit's business processes and require the immediate attention of management.

Priority 4: Important findings that need to be resolved by management.

Priority 3: The accuracy of records is at risk and requires attention.

Priority 2: Minor control issues have been identified which nevertheless need to be addressed.

Priority 1: Administrative errors identified that should be corrected. Simple, no-cost measures would serve to enhance an existing control.

Definitions of Corporate Risk

Risk	Reporting Implications
Low	Issues of a minor nature or best practice where some improvement can be made.
Medium	Issues which should be addressed by management in their areas of responsibility.
High	Issues that we consider need to be brought to the attention of senior management.
Very High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.