Argyll and Bute Council

Internal Audit Report

August 2020

FINAL

Logical Access

Audit Opinion: Reasonable

	High	Medium	Low	VFM
Number of Findings	0	2	3	0

Contents

Contact Details

Internal Auditor: Mhairi Weldon

Telephone: 01546 604294

e-mail: mhairi.weldon@arygll-bute.gov.uk

www.argyll-bute.gov.uk

1. Executive Summary

Introduction

1. As part of the 2019/20 internal audit plan, approved by the Audit & Scrutiny Committee in March 2019, we have undertaken an audit of Argyll and Bute Council's (the Council) system of internal control and governance in relation to logical access to key systems.

2. The audit was conducted in accordance with the Public Sector Internal Audit Standards (PSIAS) with our conclusions based on discussions with council officers and the information available at the time the fieldwork was performed. The findings outlined in this report are only those which have come to our attention during the course of our normal audit work and are not necessarily all the issues which may exist. Appendix 1 to this report includes agreed actions to strengthen internal control however it is the responsibility of management to determine the extent of the internal control system appropriate to the Council.

3. The contents of this report have been agreed with the appropriate council officers to confirm factual accuracy and appreciation is due for the cooperation and assistance received from all officers over the course of the audit.

Background

4. Every service the Council provides depends on data and the applications, tools and devices we use to capture, process, protect and manage it. Data is held on a wide range of subjects including service users, customers, suppliers, members of the public, council officers and properties.

5. The Council's ICT and Digital Strategy confirms that the Council has a large and complex information and technology landscape comprising:

    - 115,000 emails per day
    - 1,200 mobile phones
    - 260 applications
    - 5,000 users
    - 7,600 devices
    - 2,300 Lync/Skype Accounts
    - 400 servers
    - 93 networked schools
    - 95 networked offices.

6. The sixth data protection principle under the Data Protection Act 2018 states that "*personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)*".

7. The Council is therefore required to put appropriate policy and technology based control measures in place to ensure that the three following elements of information protection are maintained:

- Confidentiality – information should be available only to those who rightfully have access to it
- Integrity – information should be modified only by those who are authorised to do so
- Availability – information should be accessible to authorised users who need it when they need it.

8. Access to any council computer system should only be granted where there is a demonstrable business need. Logical access controls verify a user's identity mostly through the use of a unique username and password. These controls are in place to either prevent or allow access to information once a user's identity has been established. Once a user is logged in they should only have access to the information required to perform their duties.

Scope

9. As outlined in the Terms of Reference agreed with the Head of Customer Support Services on 5 December 2019, the scope of the audit was to assess key system logical access rights to ensure they are commensurate with officer responsibilities. The controls in place to provide access to the corporate network will be reviewed as will controls to access the following key systems that facilitate financial transactions that may result in payments being made by the council:

- ResourceLink Payroll
- Oracle Payables
- Open Revenues Benefits & Council Tax
- Pecos Purchasing
- SEEMIS payments
- BACS
- Northgate ORBiS Non-Domestic Rates (NDR)
- TOTAL Roads Costing System
- Tranman Fleet Management System
- Civica Financials Debtors
- ICON Cash Receipting
- CareFirst Care Charging

10. Note that the Civicia Financial Debtors system makes use of the Active Directory to facilitate logical access. This means that once a user logs in to the corporate network they can automatically log on to debtors as long as they have an established account on the debtors system. For this reason a number of the tests set out in section three of this report are not applicable to the debtors system.

Risks

11. The risks considered throughout the audit were:

- **SRR11:** Service Delivery – Cyber Security
- **Audit Risk 1:** Breach of Data Protection Act 2018 and General Data Protection Regulations (GDPR) which may result in the Council incurring financial penalties
- **Audit Risk 2:** The Council may be subject to malicious activity such as fraud, theft of data and, identify theft or attacks on systems (e.g. denial of service)

Audit Opinion

12. We provide an overall audit opinion for all the audits we conduct. This is based on our judgement on the level of assurance which we can take over the established internal controls, governance and management of risk as evidenced by our audit work. Full details of the five possible categories of audit opinion is provided in Appendix 2 to this report.

13. Our overall audit opinion for this audit is that we can take a reasonable level of assurance. This means internal control, governance and the management of risk is broadly reliable. However, whilst not displaying a general trend, there are areas of concern which have been identified where elements of residual risk or weakness may put some of the system objectives at risk.

Recommendations

14. We have highlighted two medium priority recommendations and three low priority recommendations where we believe there is scope to strengthen the control and governance environment. These are summarised below:

- procedures/user manuals for NDR, BACS and Tranman systems should include guidance on logical access controls
- generic User IDs should not be used for any system activity
- where possible password controls should be enhanced to better comply with good practice
- where possible logon controls should be enhanced to better comply with good practice
- where possible user management controls should be enhanced to better comply with good practice.

15. Full details of the audit findings, recommendations and management responses can be found in Section 3 of this report and in the action plan at Appendix 1.

2. Objectives and Summary Assessment

16. Exhibit 1 sets out the control objectives identified during the planning phase of the audit and our assessment against each objective.

Exhibit 1 – Summary Assessment of Control Objectives

	Control Objective	Link to Risk	Assessment	Summary Conclusion
1	The Council has, and complies with, appropriate policies/ procedures in relation to logical access controls.	SRR11 Audit Risk 1	Substantial	Users are required to sign an Acceptable Use Policy and be appropriately authorised before gaining network access. Some system manuals could be enhanced to provide better guidance on logical access controls.
2	Access to key systems is restricted to authorised users.	SRR11 Audit Risk 1 Audit Risk 2	Reasonable	System users are authorised by management and made aware of their responsibilities. However issues have been identified regarding generic user IDs and logical access controls not meeting good practice.
3	User access is restricted to functions commensurate with the user's job responsibilities.	SRR11 Audit Risk 1 Audit Risk 2	Substantial	Users are granted system access in line with their job requirements and managing user access is appropriately restricted to system administrators. Not all user access request forms

				were available for review and there is a lack of audit trails in three systems.
4	System administrators are notified of role changes and leavers promptly.	SRR11 Audit Risk 1 Audit Risk 2	Reasonable	All systems have processes to report user changes and leavers however notifications are not always received in a timely manner. User rights and permissions are not formally reviewed in all systems.

17. Further details of our conclusions against each control objective can be found in Section 3 of this report.

3. Detailed Findings

The Council has, and complies with, appropriate policies/procedures in relation to logical access controls

18. The Council has an Acceptable Use Policy (AUP) that is designed to promote the integrity, security, reliability and privacy of the Council's information systems, electronic communications and networks and networks to which they connect. The AUP applies to all employees, elected members, contractors, consultants, temporary staff and employees of partner organisations such as LiveArgyll and the Health and Social Care Partnership. Formal acceptance of the AUP and authorisation by an appropriate officer must be submitted to ICT as a condition of being granted access to the Council's IT resources and being allocated an internet/email account.

19. The AUP was last reviewed in December 2018 and includes guidance on password selection and non-disclosure and outlines accountability for actions linked to a user's login ID.

20. User access request forms for a random sample of 30 network users were reviewed to ensure they were fully completed, signed by the user and authorised by an appropriate officer. Forms submitted since mid-2017 were stored electronically and easily located. Hard copies of older forms were filed in lever arch files. All were located bar one for which there were notes on the previous ICT helpdesk system that indicated the form had been received and appropriate actions had been taken to enable the employee to access the network. All 29 reviewed had been appropriately completed and signed by the user, however one was not authorised. On further investigation we confirmed this one was part of a batch submitted by a school where all the forms had been completed and signed by the users but none had been authorised. This is considered an isolated incident and so no audit issue has been raised.

21. Compliance with the AUP is predominantly enforced through embedded network and system controls. Alerts are set up to flag attempts to circumvent these controls with logs maintained to review unauthorised access attempts. An annual password audit is carried out using a similar tool that a hacker might use. If any passwords are successfully hacked during this test the user is contacted and advised to change their password and reminded of good password practice. This was last carried out in August 2020 and we have been advised that, going forward, it will be performed quarterly.

22. Procedures or user manuals were provided for each of the twelve systems outlined in paragraph nine. Eight included guidance regarding logical access controls, but there was no logical access guidance included in the remaining four with one of these being the debtors system which uses

the Active Directory to facilitate access. The three systems where guidance could be improved are NDR, BACS and Tranman.

Action Plan 1

Access to key systems is restricted to authorised users

23. Users are made aware of their system responsibilities through a combination of documented guidance, in-house training and mentoring. There is also a misuse deterrent statement displayed at initial network logon stage. A similar deterrent is not displayed when logging in to individual systems however this is not considered necessary as the network statement is considered sufficient.

24. Users require management authorisation to gain access to systems. This can be provided either by completing a form or by sending an email directly from the authorising officer stating the user role and level of access required. There is also a formal process in place for consultants to obtain time restricted remote access to council systems to install upgrades and patches or resolve any reported issues. Five of the systems have generic IDs to provide remote access to consultants and five have no generic IDs. The remaining two systems share user IDs to facilitate system administrator activity. (Exhibit 1)

Action Plan 2

25. When users log into the network, and each of the systems, passwords are hidden to prevent disclosure to unauthorised users. Users are prompted to change their password when logging in for the first time for all but three systems. Password change is not enforced in the NDR system although this can be activated, users are currently advised to change passwords manually and the Tranman system does not have the required functionality to allow password changes. Seven systems prevent re-use of older passwords however this control can be activated in a further three systems. (Exhibit 1)

26. Good password selection is essential in maintaining the security of user accounts. A greater number of enforced requirements (complexity) will increase the number of possible combinations of letters, numbers and other characters making it more difficult for an unauthorised user to guess or hack passwords. Password complexity is enforced by the Council's network and by five of the systems, it can be activated in the payroll system, however, it is not working within Pecos. The control is not currently available in the three remaining systems which place reliance on network access controls as the systems cannot be accessed without first logging onto the network. (Exhibit 1)

Exhibit 1: Summary of Password Testing

System	Payroll	CareFirst	Open Revenues	NDR	Cash Receipting	BACS	Sundry Debtors	Oracle Payables	PECOS	SEEMIS EMA	TOTAL	Tranman
Generic IDs used (C=Consultant; SA=Systems Admin)	C	C	C	SA	C	N	N/A	N	SA	-	C	-
Password change on first login	Y	Y	Y	N	Y	Y	N/A	Y	Y	Y	Y	N
Can re-use old passwords	N	Y	N	Y	N	N	N/A	Y	N	N	N	N/A
Password complexity enforced	N	N	Y	N	Y	Y	N/A	N	N	Y	Y	N

Action Plan 2 and 3

27. When a user inputs an incorrect username or password a system message advises them of an error but not which is incorrect. Repeated invalid login attempts will result in the user account being locked by eight of the systems. The control has been activated in Oracle Payables, however it is not working, and therefore there is no restriction on the number of failed attempts for three systems. System users are unable to view when they last logged onto the system, however this information can be accessed by systems administrators for five of the systems. (Exhibit 2)

28. A controlled log-off is enforced in eight of the systems if the user is inactive for a specified number of minutes however, for two, the period is in excess of an hour and the remaining four do not log a user off after a period of inactivity. Reliance is largely placed on the lock screen facility within the windows desktop operating system to provide some risk mitigation, however, it was found that settings for this could be adjusted by the end user on some devices. Windows screen saving and power saving settings have been revised and testing carried out confirms that the screen will go blank following a period of 10 to 12 minutes of inactivity, following this the user must re-enter their network credentials to regain access to the screen.

29. Payroll and SEEMIS systems automatically disable a user if they do not access the system for 28 or 60 days respectively. For four systems a manual exercise is undertaken at various intervals to identify inactive accounts. For the remainder there is no review of inactive accounts carried out. (Exhibit 2)

Exhibit 2: Summary of Logon Testing

System	Payroll	CareFirst	Open Revenues	NDR	Cash Receipting	BACS	Sundry Debtors	Oracle Payables	PECOS	SEEMIS EMA	TOTAL	Tranman
Failed logins lock user account	Y	N	Y	Y	Y	Y	N/A	N	Y	Y	Y	N
Time of previous login available	Y	N	N	N	N	N	N	Y	N	Y	Y	Y
Controlled logoff enabled	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N
Inactive users disabled	Y	Y	N	Y	N	N	Y	Y	N	Y	N	N

Action Plan 4

User access is restricted to functions commensurate with the user's job responsibilities

30. Access to create, amend, disable or delete users is restricted to appropriately appointed systems administrators for all twelve systems.

31. User roles are set up within systems to allow users with similar job requirements to access a specific set of menus aligned to their job role. All systems are able to tailor menus assigned to user roles and these are considered to be suitable for work requirements. Some users will have more than one role and, in these instances, they will be able to switch roles within the system or by exception have more than one user ID.

32. A sample of four users for each of the twelve systems was reviewed to ensure an appropriately authorised request had been received instructing the user to be added to the system. All access forms or emails requesting access were provided for six systems, partially provided for four systems and unavailable for the remaining two systems. There were a variety of reasons for this including users added as part of original system set-up, changes in record storage and inability to access paper records due to COVID related access restrictions to buildings. Completed forms for SEEMIS are not retained. All system users reviewed had been granted appropriate system access that is commensurate with their job role. (Exhibit 3)

33. Systems contain a data file holding user passwords that are used to validate user logins. This file should be encrypted and not accessed unless in exceptional circumstances. This file is hidden or encrypted within eleven of the systems and therefore unavailable even to systems administrators. The password file within the remaining system can be viewed by the systems administrator who creates and allocates the password to the user. (Exhibit 3)

34. Audit trails chronologically record transactions that are processed on a system and can be used to verify actions taken and trace errors or other anomalies. Audit trails were found to be available for ten systems either through the main system or the associated workflow/document management system. Limited information is available for the Oracle payables system which only provides information relating to record creation and the last record update with the history of all other changes not retained. Tranman does not provide any audit trail. (Exhibit 3)

System administrators are notified of role changes and leavers promptly

35. All twelve systems were found to have manual processes in place to report user changes and leavers, however, for seven of these systems, we were advised that notifications were not always received in a timely manner. Where systems are operated within small teams the systems administrator is aware of any changes and leavers and these are acted upon immediately. (Exhibit 3)

36. Regular review of user rights and permissions to ensure system access remains appropriate and adequate separation of duties is maintained is in place for seven systems. For the remaining systems there is no formal periodic review although for three there may be reviews carried out on an ad hoc basis. (Exhibit 3)

Exhibit 3: Summary of User Management Testing

System	Payroll	CareFirst	Open Revenues	NDR	Cash Receipting	BACS	Sundry Debtors	Oracle Payables	PECOS	SEEMIS EMA	TOTAL	Tranman
Access appropriately authorised	Y	P	P	P	Y	N	Y	P	Y	N	Y	Y
Password file encrypted/hidden	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Audit trails available	Y	Y	Y	Y	Y	Y	Y	P	Y	Y	Y	N
Changes/leavers notified timely	N	Y	N	Y	N	Y	N	Y	N	Y	N	N
User rights/permissions reviewed	Y	Y	P	Y	P	P	Y	Y	Y	Y	N	N

(Y=Yes; P=Partial; N=No)

Action Plan 5

Appendix 1 – Action Plan

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	1	**Procedures/User Manual** Procedures/user manuals for the NDR, BACS and Tranman systems do not provide any guidance on logical access controls.	Logical access controls may be insufficient to provide robust system security.	NDR – User Manual will be updated to include guidance on logical access controls. BACS – guidance on logical access controls will be provided to users. Tranman – Civica have advised that there may be an option to make use of Active Directory to access the system and this is being considered.	Systems Administrators NDR 30 September 2020 BACS 30 September 2020 Tranman 31 March 2021

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
Medium	2	**Generic User IDs** The NDR & PECOS systems have a generic User ID which is used to carry out system administration.	Activity undertaken using generic IDs cannot be traced to the correct officer.	NDR – Adjustments have now been made to allow supervisory staff to access system administration duties using separate IDs. PECOS - Cannot be resolved. The Pecosadmin user ID provides access to the system inbox to receive notification of issues that must be resolved quickly to allow processing to continue. This prevents notifications going into an individual's inbox and failing to be addressed in the event of absence.	Systems Administrators Complete N/A

Low	3	**Password Controls**
		
		A number of issues were identified where password controls fell short of good practice. In some circumstances the systems do not have the required functionality. We have only highlighted issues where the system does have the functionality however it has not been turned on.
		
		• Non Domestic Rates
		  ○ Password changes are not enforced
		  ○ Old passwords can be reused
		• Oracle Payables
		  ○ Old passwords can be reused
		  ○ Password complexity not enforced
		• Carefirst
		  ○ Old passwords can be reused
		  ○ Password complexity not enforced
		• Payroll
		  ○ Password complexity not enforced
		• Tranman
		  ○ Password changes are not enforced
		  ○ Password complexity not enforced
		  ○ Password file visible to the systems administrator
		• PECOS
		  ○ Password complexity is switched on but not working
			Unauthorised users may gain access to systems.	NDR – ICT have now installed updates that enforce password change and prevent re-use of recent passwords.
				
				Oracle Payables – This will be addressed in forthcoming upgrade/new system.
				
				CareFirst – On 21 August a call was logged with OLM asking if the relevant configurations can be amended.
				
				Payroll – Password complexity will be introduced by end of December 2020.
				
				Tranman – Civica have advised that there may be an option to make use of Active Directory to access the system and this is being considered.
					Systems Administrators
					
					NDR
					Complete
					
					Oracle Payables
					30 June 2022
					
					CareFirst
					Resolution and timescale will depend on response to logged call
					
					Payroll
					31 December 2020
					
					Tranman
					31 March 2021

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
				PECOS – On 20 July 2020 a call has been logged with Elcom regarding the fault.	PECOS Resolution and timescale will depend on response to logged call

Low	4	**Logon Controls**
		
		A number of issues were identified where logon controls fell short of good practice. In some circumstances the systems do not have the required functionality. We have only highlighted issues where the system does have the functionality however it has not been turned on.
		
		• Oracle Payables
		  ○ Locking user after failed login attempts switched on but not working
		• Carefirst
		  ○ Inactive user logoff exceeds one hour
		• Tranman
		  ○ User not locked following failed login attempts
		  ○ No control over inactive users
		• PECOS
		  ○ No control over inactive users
		• Debtors
		  ○ Inactive user logoff exceeds one hour
		• Open Revenues
		  ○ No control over inactive users
		• Cash Receipting
		  ○ No control over inactive users
		• BACS
		  ○ No control over inactive users
		• TOTAL
		  ○ No control over inactive users
			Unauthorised users may gain access to systems.	Oracle Payables – In July 2020 a call was logged with supplier to address this fault.
				
				CareFirst – system does not recognise typing as an activity and therefore cannot reduce the inactive session timeout limit.
				
				Tranman – Civica have advised that there may be an option to make use of Active Directory to access the system and this is being considered.
				
				PECOS – An annual review of inactive users will be implemented.
				
				Debtors – Active session timeout will be amended to 15 minutes and reviewed to ensure this does not create operational issues.
					Systems Administrators
					
					Oracle Payables
					Resolution and timescale will depend on response to logged call
					
					CareFirst
					N/A
					
					Tranman
					31 March 2021
					
					PECOS
					31 January 2021
					
					Debtors
					Complete

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
				Open Revenues – System supplier will be asked if a solution is possible to address issues identified. Cash Receipting – System supplier will be asked if a solution is possible to address issues identified. BACS – System supplier will be asked if a solution is possible to address issues identified. TOTAL – A manual exercise will take place to review inactive users and will repeat annually.	Open Revenues 30 September 2020 Cash Receipting 30 September 2020 BACS 30 September 2020 TOTAL 31 December 2020

Low	5	**User Management Controls**
		
		A number of issues were identified where user management controls fell short of good practice. In some circumstances the systems do not have the required functionality. We have only highlighted issues where the system does have the functionality however it has not been turned on.
		
		• Oracle Payables
		  ○ Audit trails are limited
		• Tranman
		  ○ Leaver and change notifications are not always received in a timely manner
		  ○ No review of user access rights and permission levels
		  ○ No audit trail is available
		• PECOS
		  ○ Leaver and change notifications are not always received in a timely manner
		• Debtors
		  ○ Leaver and change notifications are not always received in a timely manner
		• Open Revenues
		  ○ Leaver and change notifications are not always received in a timely manner
		  ○ A review of user access rights and permission levels takes place on an ad-hoc basis
		• Cash Receipting
		  ○ Leaver and change notifications are not always received in a timely manner
		  ○ A review of user access rights and permission levels takes place on an ad-hoc basis
			Users may not have been appropriately authorised to gain access to the system or may retain access to privileged information when no longer required.	Oracle Payables – Audit trails will be addressed in forthcoming upgrade/new system
				
				Tranman – on 25 august a call was logged with Civica regarding audit trail.
				
				Change and leaver reminder will be issued and user access rights and permission levels will be reviewed annually.
				
				PECOS – Intend to work with HR to create a report to identify leavers and changes.
				
				Debtors – Reminders will be issued to supervisors twice yearly to advise of leavers and changes.
				
				Open Revenues – Staff will be reminded to advise of changes and leavers in a timely manner. Although ad-
					Systems Administrators
					Oracle Payables
					30 June 2022
					
					Tranman
					Resolution and timescale will depend on response to logged call
					
					31 March 2021
					
					PECOS
					31 December 2020
					
					Debtors
					30 September 2020
					
					Open Revenues
					30 September 2020

		• BACS
		  ○ A review of user access rights and permission levels takes place on an ad-hoc basis
		• SEEMIS
		  ○ Access forms or emails requesting access are not retained
		• TOTAL
		  ○ Leaver and change notifications are not always received in a timely manner
		  ○ No review of user access rights and permission levels
		• Payroll
		  ○ Leaver and change notifications are not always received in a timely manner
				hoc, user reviews do take place annually.
				
				Cash Receipting – Staff will be reminded to advise of changes and leavers in a timely manner. Although ad-hoc, user reviews do take place annually.
				
				BACS – Staff will be reminded to advise of changes and leavers in a timely manner. Although ad-hoc, user reviews do take place annually.
				
				SEEMIS – Copies of authorised requests for access to EMA and Clothing Grants module will be retained in future.
				
				TOTAL – Reminders will be issued by email to advise that leavers and changes must be notified. The monthly post detail report will also be checked.
					
					Cash Receipting
					30 September 2020
					
					BACS
					30 September 2020
					
					SEEMIS
					30 September 2020
					
					TOTAL
					30 September 2020

	No	Finding	Risk	Agreed Action	Responsibility / Due Date
				A manual exercise will take place to review access rights and will repeat annually. Payroll – This will be considered as part of the current BPR exercise being carried out.	31 December 2020 Payroll 31 December 2020

In order to assist management in using our reports a system of grading audit findings has been adopted to allow the significance of findings to be ascertained. The definitions of each classification are as follows:

Grading	Definition
High	A major observation on high level controls and other important internal controls or a significant matter relating to the critical success of the objectives of the system. The weakness may therefore give rise to loss or error.
Medium	Observations on less significant internal controls and/or improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system. The weakness is not necessarily substantial however the risk of error would be significantly reduced if corrective action was taken.
Low	Minor recommendations to improve the efficiency and effectiveness of controls or an isolated issue subsequently corrected. The weakness does not appear to significantly affect the ability of the system to meet its objectives.
VFM	An observation which does not highlight an issue relating to internal controls but represents a possible opportunity for the council to achieve better value for money (VFM).

Appendix 2 – Audit Opinion

Level of Assurance	Definition
High	Internal control, governance and the management of risk are at a high standard. Only marginal elements of residual risk have been identified with these either being accepted or dealt with. A sound system of control designed to achieve the system objectives is in place and being applied consistently.
Substantial	Internal control, governance and the management of risk is sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Reasonable	Internal control, governance and the management of risk are broadly reliable. However, whilst not displaying a general trend, there are areas of concern which have been identified where elements of residual risk or weakness may put some of the system objectives at risk.
Limited	Internal control, governance and the management of risk are displaying a general trend of unacceptable residual risk above an acceptable level and placing system objectives are at risk. Weakness must be addressed with a reasonable timescale with management allocating appropriate resources to the issues raised.
No Assurance	Internal control, governance and the management of risk is poor. Significant residual risk and/or significant non-compliance with basic controls exists leaving the system open to error, loss or abuse. Residual risk must be addressed immediately with management allocating appropriate resources to the issues.