Systems Review Action Plan: Action Plan: Payroll 2010-11 S.044.11					**Action Plan 1**	
Date Issued :						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
1.	**No Date Stamp** From a sample of 15 leavers and 15 transfer forms tested, it was noted that 4 leavers forms and 2 transfer forms were not date stamped.	All documentation received by the Payroll Office should be date stamped to evidence date of receipt.	Low Risk	Staff will be reminded to date stamp all mail received. A spot check will be done to ensure that this is being carried out.	Sam Dove Section Head – Workforce Planning & Resourcing	4.4.11
2.	**Authorised Signatories** Departmental Authorised Signature Records could not be found for 4 of the sample of 15 leavers forms tested.	Documentation should only be processed and amendments made to payroll where a specimen signature is provided and checked to Authorised Signature Records. A request should be made as soon as possible to HR for an up to date list of all HR staff authorised to sign specified documents.	Medium Risk	An up to date list of authorised signatories will be compiled as soon as possible and thereafter held on file.	Sam Dove Section Head – Workforce Planning & Resourcing	28.4.11
3.	**Authorisation of Payroll Amendments** From the sample of 15 leavers forms tested, 1 of the forms had been authorised by the Lead HR Advisor (Pay Provision) who is involved in the development of the new System, and is not an authorised signatory.	It is recommended that System Development/Payroll staff do not authorise any HR documentation relating to amendments to Payroll.	Medium Risk	This was done as a one off at that time in the development of the live system.	Sam Dove Section Head – Workforce Planning & Resourcing	1.4.11

Systems Review Action Plan: Action Plan: Payroll 2010-11 S.044.11						Action Plan 1	
Date Issued :							
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**	
4.	**PYOL (Payroll Forms)** Payroll staff update the payroll system and record their initials and the date on the PYOL forms, where applicable this is checked by a senior member of staff and they also record their initials and date. However there is no place on the PYOL form for these details to be formally recorded.	The PYOL form should be modified to include a section which can be utilised by Payroll staff to record their details as appropriate.	Low Risk	The form will be adapted to include a Section for Payroll staff to record their initials and date.	Sam Dove Section Head – Workforce Planning & Resourcing	28.4.11	

Systems Review Action Plan: Planning Applications 2011-12 S.001.12					**Action Plan 2**	
Date Issued : July 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
1.	**Income Checks** A report is produced from the planning database on a weekly basis showing all new applications and the details are checked to the daily income sheets to ensure bankings are correct. However, the report is not signed as approved by the officer carrying out these checks.	The officer responsible for carrying out the checks should sign the reports as evidence of approval.	Low Risk	The weekly report is now being signed and dated by the officer carrying out the checks from 11/7/11.	Pamela Clifford Planning & Building Standards Manager	1.7.11
2.	**Mis-Filed Documents** A sample of 30 Planning Applications was selected for testing and the electronic files for each application were examined. From the sample tested documentation relating to other planning applications for 3 of the test sample were found to have been scanned and mis-filed.	Planning Officers should be reminded to check files for erroneous documents and where identified, re-index prior to passing to the Team Leader for a decision.	Low Risk	Staff will be reminded to check files, and will be reminded again whenever misfiled documents are found, e-mail sent to all Planning and Support staff 8/7/11.	Pamela Clifford Planning & Building Standards Manager	8.7.11
3.	**Validation Letters** From the same sample of electronic files examined as above, it was noted that validation letters for 2 of the test sample were not held on file nor had they been printed and issued to applicants.	Where an application is valid, validation letters should always be issued, which provides the applicant with statutory information and ensures that performance figures are accurate.	Medium Risk	Staff will be reminded of the importance of issuing validation letters at the same time as the application is recorded as valid on the CAPS system, e-mail sent to all Planning and Support staff 8/7/11.	Pamela Clifford Planning & Building Standards Manager	8.7.11

Systems Review Action Plan: Planning Applications 2011-12 S.001.12					Action Plan 2	
Date Issued : July 2011						
Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
4.	**Authorisation of Refunds** A sample of 5 refunds was selected for testing. It was noted that the Planning Administration Officer prepares and authorises a 'Planning Application Refund Request' at the verbal request of a Planning Officer. However there is no written authorisation from the Planning Officer or senior employee.	The 'Planning Application Request' form should be adapted to include a section where the Planning Officer or senior employee can sign and date the form as the authoriser. The Planning Administration Officer should sign and date as the preparer.	Medium Risk	The form has now been amended to incorporate the additional signature and date and is in use from 11/7/11.	Pamela Clifford Planning & Building Standards Manager	11.7.11
5.	**Refunds - Covering Letter** Refund cheques are issued directly from Creditors without a covering letter explaining the reason for the refund.	Where a refund is to be issued, the applicant should be informed of the reason for the refund. Therefore a standard letter should be issued advising of the amount/details and that a cheque will be issued under separate cover.	Low Risk	Standard letter templates will be modified to cover all situations and to include a clear statement that the cheque will follow under separate cover and will be in use from 25/7/11.	Pamela Clifford Planning & Building Standards Manager	25.7.11
6.	**Reconciliations** Checks are not being undertaken to ensure that income is being banked and coded appropriately to the Financial Ledger.	Monthly checks should be carried out by checking the receipts issued to the daily income sheet and then checking the daily income totals to the financial ledger postings. This should be carried out by an independent	Medium Risk	A monthly report will be issued to the Management Accountant providing the relevant information in order that reconciliations can be performed.	Pamela Clifford Planning & Building Standards Manager	1.7.11

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
Systems Review Action Plan: Planning Applications 2011-12 S.001.12 **Date Issued : July 2011**					**Action Plan 2**	
		officer who should sign and date the ledger prints as evidence that the checks were carried out.				

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)						Action Plan 3
Date Issued : March 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	1.1 Saffron Ownership Our review considered the strategic development and corporate ownership of the Saffron system. During discussions with senior users of the system and ICT, we noted that ownership of the Saffron system rested solely with ICT. There is no evidence that HEED had any strategic or day to day ownership of the system and its data. There is a risk that this lack of ownership could result in the Council not fulfilling strategic objectives. There is also a risk that this creates an overreliance on Civica, the system supplier.	We recommend that management ensure that ownership of the Saffron system is allocated to HEED. Senior management within the department should be responsible for making key decisions regarding strategic decisions for the development and operation of the system. Grade 3		Agreed – current named HEED Service Manager is Janice Lockhart, Homelessness and Allocations Manager A key element in the ICT Securitisation Project Option Appraisal is the replacement/renewal of Saffron which will be examined as an integral part of that project. **To be actioned by:** Helen Turley, Head of Housing and Community Safety & Patricia Marshall, ICT Manager **No later than:** To be determined by the prioritisation of the Securitisation Project.		
	1.2 Procedures Manuals					

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)					**Action Plan 3**	
Date Issued : March 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	During discussions with module users, we found that administrative procedures around Saffron were well developed. System documentation was available to users and some teams using Saffron had developed their own internal manuals to assist with day-to-day operation of the system. Procedures in relation to user access and user creation are maintained by ICT and are readily available. We noted, however, that some documentation was more than 15 years old and referred to earlier versions of Saffron. In addition, documentation does not exist for all system modules. It was noted that new members of staff rely on instruction from common practices of colleagues rather than by reference to procedural documentation. There is a risk that the lack of internal procedural manuals for each Saffron module could result in inconsistent practices within teams.	We recommend that procedural manuals for each module of Saffron are produced in order that the use of each module is standardised within the teams managing the module. This will assist with training new staff. We also recommend that the existing procedures are subject to regular review and update to confirm that they are consistent with current working practices. Grade 2		**Rent Accounting** The Revenues & Benefits Section will ensure all procedures manuals in use are the most recent version and will carry out a review of existing procedures. **To be actioned by:** Marion Smith, Section Head Revenues & Benefits **No later than:** 30th September 2011 **Housing** The Housing and Community Safety Service will develop a comprehensive procedure manual once the housing allocations staff are co-located. **To be actioned by:** Janice Lockhart, Homelessness & Allocations Manager **No later than:** 31st March 2012		
	1.3 Knowledge Transfer During discussions with senior module users, we noted that, due to retrials and staff reallocations,					

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	users with significant knowledge of the system are no longer available to support the day to day operation of the system. We noted that there has not been any formal process to ensure that there was appropriate knowledge transfer. When meeting with one senior user, we noted that there was limited handover and knowledge transfer to the member of staff who was inheriting their responsibilities. There is a risk that the Council will have an increasing reliance on Civica for support to resolve user queries. This may result in delays in processing and resolving user queries as well as increasing processing time.	We recommend that management ensure that they seek to reduce overreliance on key personnel. In addition, where it is known that a key member of staff will be leaving the Council, management should ensure that a formal handover process is agreed so that there is appropriate knowledge transfer. Where possible and practical, documentation should be prepared to support this process. Grade 3		**Rent Accounting** The restructure of the Revenues & Benefits Section in October 2010 sought to address over reliance on key personnel particularly on the systems side. All major processes are documented and able to be carried out by several members of the support & continuous improvement team. **Housing** It is acknowledged that key personnel have left the service. There is confidence that the ICT provider is able to continue to support and upgrade the system as appropriate, but it is important that internal users are qualified to maintain the IHMS. **To be actioned by:** Helen Turley, Head of Housing and Community Safety & Patricia Marshall, ICT Manager **No later than:** 31st March 2012		
2.1 Third Party Access During our review, we were informed that the software supplier, Civica, obtains access to the system for patching, updates and systems modifications. Access to	We recommend management ensure that		Remote Access procedures are currently under		

Date Issued : March 2011

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	the system is granted by the Council on receiving the appropriate authorised Change Request. After granting access, ICT will reset the password after a brief interval to prevent the password being reused. Unless specifically agreed, Civica's access is set to automatically expire at close of business. We noted from discussions with senior ICT personnel that when remote access is permitted, they activate the group containing Civica accounts. This activates all accounts within that group. This means that, as has occurred in the past, several Civica programmers can access Saffron simultaneously, despite approval only being given for a single access. Civica has been reminded that only one user should be logging in at a time, however, the current process to activate the group rather than individual user accounts does not prevent this. There is a risk that the current process of granting Civica remote access to the Saffron system does not prevent multiple accesses by Civica to the system. This could result in unauthorised changes being made.	when Civica require remote access to the Saffron system they activate individual user accounts rather than groups of accounts. This will prevent uncontrolled access by Civica to the Council's network and the Saffron system. Grade 4		review. Civica have been contacted with our proposal to implement individual user accounts to their engineers and consultants who require access to WDC's network and Saffron application. **To be actioned by:** John Martin, Section Leader ICT Connect **No later than:** 31st December 2011		

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)					**Action Plan 3**	
Date Issued : March 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	2.2 Powerful account passwords We noted that ICT maintains a book to record the passwords of powerful user accounts. Access to the book is restricted to the four members of the ICT Server Team. The book is held in a secure cabinet and we noted the room was locked when the room was left unattended. We noted that this contains the passwords for the majority of UNIX and Windows servers, including the root password for the Saffron UNIX environment. We noted that records are not maintained to record who had access to the password list nor were passwords changed following access. There is a risk that changes made using powerful accounts cannot be attributed to a named individual.	We recommend that all access to passwords is formally recorded so that there is an appropriate audit trail to identify individual access to accounts. We also recommend that whenever use of the accounts is completed, passwords are immediately changed. We recommend that management ensure that access to the password book is restricted and accessible only to a trusted individual. Where the Administrator password is required this should be requested from the trusted party. We also recommend that secure password access procedures are used where the trusted individual is not available. To be effective this should require that passwords can only be viewed or accessed on an individual basis. Grade 3		An investigation into a number of password management tools (e.g. password manager pro) is taking place. A capital bid will be submitted in FY 2011/12 for a security tool to manage WDC passwords. Procedures will be reviewed and amended to include an audit trail, facilitate passwords being held via a password management tool and restrict access to trusted users. **To be actioned by**: Brian Miller, Section Leader ICT Infrastructure **No later than:** 31st March 2012		
	2.3 Account Lockout					

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	We noted that automatic login to powerful system accounts is disabled in the UNIX system, with users having to login manually using the Switch User ("su") command to the powerful account. This ensures that there is an audit trail for use of the account. While recognising that there are enforced password changes on a periodic basis, we noted that there is currently no functionality within Saffron or UNIX that will lock user accounts where a user fails to login to the system after a pre-defined number of attempts. There is a risk that unauthorised users are able to make repeated and sustained attempts to gain access to user accounts without the account being locked. This risk is increased as audit trails are not enabled to support the detection of such attempts.	We recommend that management liaise with Civica to establish whether account lockout functionality can be enabled. If so, management should ensure that accounts are set to lock after no more than 5 failed login attempts. Furthermore, management should also ensure that accounts can only be unlocked by a member of ICT. We also recommend that management ensure audit logs are enabled so that successful and unsuccessful login attempts are recorded. These should be reviewed on a daily basis to gain assurance that there have not been any attempts to gain unauthorised access to the system. Grade 3		Agreed. **To be actioned by:** John Martin, Section Leader ICT Connect **No later than:** 31st March 2012		

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff) **Action Plan 3**
Date Issued : March 2011

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)					**Action Plan 3**	
Date Issued : March 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	2.4 Antivirus We noted that anti-virus software is not installed on the UNIX server estate supporting the Saffron system. Whilst appreciating that UNIX viruses are rare, there has been a small number of incidents of viruses infecting UNIX systems. As UNIX access is via a Microsoft Windows application, there is a risk that a virus could be introduced to one OS from the other.	We recommend management perform a risk assessment to determine the value of installing virus scanning software in the UNIX server estate supporting the Saffron system. Grade 2		Agreed. **To be actioned by:** Brian Miller, Section Leader ICT Infrastructure **No later than:** 31st December 2011		
	3.1 New User Creation					

| Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff) | | | | | **Action Plan 3** | |
| Date Issued : March 2011 | | | | | | |
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	During our review, we noted that all users must be created via a Helpdesk request, which requires sign-off by the user's Line Manager. New users also have to sign ICT confidentiality agreements. Only after the user has confirmed acceptance of the ICT security policy and the User Creation Form has been signed off by a line manager and submitted to the Helpdesk are users granted access to the system by the Server Team. A review of User Request Forms found that a number of forms did not have all relevant sections completed. For example, reason for the request, the urgency of the request and the action taken to complete the request were not always recorded. There is a risk that the absence of the information may lead to requests not being assigned the correct priority. This could result in delays to the creation of user accounts.	We recommend that line managers are reminded to include all relevant information within User Creation Forms. In addition, ICT management should remind staff to ensure that all forms are annotated with the action taken so that there is clarity in respect of whether the request has been dealt with. Grade 2		Line Managers have been reminded to include all relevant information within user creation forms. Agreed. Note: there is already a cross reference with service desk system journal entries which compliment the physical form and often have clarification statements. **To be actioned by:** John Martin, Section Leader ICT Connect **No later than:** 30th September 2011		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)
Date Issued : March 2011

Action Plan 3

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	3.2 Leavers During our audit, we were informed that a regular review of Saffron users and leavers was performed. When an employee leaves the Council, their Supervisor is expected to notify the Helpdesk team so that access is revoked. ICT also sends a list of all users who have not logged into Saffron in the preceding 30 days to all Supervisors. HR also produces a monthly report of leavers which is verified against UNIX and Saffron accounts. ICT will then take the appropriate action. If no Helpdesk call has been made, Supervisors are contacted to remind them to make the call. Our review identified one employee who had left the previous month but who retained an active account. Discussions with staff indicated that ICT had sent out the list of users to each department but the return from the line manager did not highlight that the user had left the Council. There is a risk of user accounts remaining active on the system after leaving the Council or the Saffron user group, potentially allowing unauthorised access to the system.	We recommend that management remind line managers of their responsibility to notify ICT of all users who leave the employment of the Council so that their access to the network and Saffron is revoked as soon as possible. We also recommend that management consider performing a secondary review to confirm that the accounts of all leavers are revoked. Grade 3		Agreed. All Service Managers in H&CS reminded of the importance of ensuring that there is no unauthorised access to the system. A secondary review will be carried out the first working day after an employee leaves WDC to ensure that access has been revoked. **To be actioned by:** Helen Turley, Head of Housing and Community Safety **No later than:** 1st September 2011		
	4.1 User Access					

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	We observed that access to Saffron requires approval from a user's Line Manager and is then submitted to the ICT Helpdesk. An ICT Request Form must be completed for this. Requests are reviewed for appropriateness and the Line Manager asked to verify the request if access appears excessive. For changes to access privileges, the forms do not state whether the change adds to existing privileges, or replaces them. The Server Team will verify this with the user's Line Manager. For members of staff who transfer to other HEED departments or elsewhere in the Council, ICT is not always notified, meaning that users may retain inappropriate access to Saffron. While recognising that there is a monthly report issued to Line Managers for review of active system users, there remains a risk that a user may have inappropriate access to Saffron until the report is returned and any required changes implemented.	We recommend that the ICT Request Form is amended to improve clarity over whether the changes are additional access rights or replacement access rights. We also recommend that line managers/ Supervisors are reminded to notify ICT of staff transfers so that members of staff who no longer require access to Saffron have their access revoked. Grade 3		ICT Request form will remain unchanged however, ICT Service Desk staff will request clarification where insufficient information is provided on additional access rights or replacement access rights. **To be actioned by:** John Martin, Section Leader ICT Connect **No later than:** 31st August 2011 **Housing** Agreed. **To be actioned by:** Helen Turley, Head of Housing and Community Safety **No later than:** 31st August 2011		
	6.1 Interfaces Data is transferred between Saffron and other					

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	Council systems (e.g. CARS). The interfaces were designed by Civica and the other system providers. The Server Team has created scheduled jobs to perform the required import and export routines between the system interfaces. We noted that some modules, such as the Homeless module, require that the data is processed twice. There is no reconciliation performed to validate the accuracy of this dual input. There is a risk that the lack of reconciliations between modules that require manual input could lead to erroneous data being imported and inaccurate reporting.	We recommend management investigate whether a direct interface can be made between core Saffron modules and the Homeless module to minimise duplication of effort and incidence of error caused by manual input. Grade 3		The service has appointed two key members of the Housing Policy Team, and this review is part of their responsibilities. **To be actioned by:** Helen Turley, Head of Housing and Community Safety **No later than:** 1st September 2012		
	7.1 Rent Data Rent increases are processed annually, following agreement by the Council. The changes are input	We recommend that the input and				

Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	into Saffron by uploading an internally generated file to the Test environment. The results of this are exported from Saffron and a sample of 2% of rent accounts is manually checked to ensure that the data has been correctly processed. Once this is agreed, the file is then uploaded to the Live environment. We noted that approval of the changes was performed within the Rents team, often by the person responsible for inputting the data. There was no evidence of a senior manager reviewing or verifying the data entry. We also noted that the exporting of rent information is to a text file, rather than a spreadsheet to perform the check. It was stated that the format of the exported file makes it too large to fit into a spreadsheet. This therefore means that checks have to be performed manually. There is an increased risk that the lack of independence in reviewing revised rent charges and low number within the sample could result in errors not being detected. This could result in negative publicity for the Council and significant remedial work.	checking of revised rent charges are performed independently. Approval of the revised rent charges to be uploaded to the live environment should be approved by a senior manager within Rents. We also recommend that management seek to use an automated solution to verify the accuracy of revised rent charges. For example, we recommend that the structure of the exported file is reviewed. The number of properties and rent amounts should make it possible to fit all information on to a spreadsheet, allowing all rents to be validated and reducing the risk of errors in the calculations. Grade 3		All rent increases will be authorised by a senior officer within the Revenue & Benefits section prior to uploading into the live environment. We will review our processes and use an automated solution to verify the accuracy of revised rent charges. **To be actioned by:** Marion Smith, Section Head Revenues & Benefits **No later than:** 31st January 2012 (time of rent increase)		
	7.2 Free Weeks The Council has a policy of allowing tenants five weeks "free" rent. Rentals for properties are, therefore, calculated over 47 weeks. Payments	We recommend that the Council seeks		Although the council has a policy to charge		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	made by Direct Debits are, however, taken over the whole year, either weekly, 4-weekly or monthly. As an example, if the annual rental on a property is £2,600, the tenant will have a weekly rental figure of £55.32. The weekly Direct Debit, however, will be for £50. As a result, Saffron cannot use the weekly rent figure to calculate the Direct Debit payment. The actual amount to be collected from tenants has to be manually calculated and input to the system. We noted that there is no audit trail or paperwork maintained to support the calculations. This is a highly time consuming and inefficient process. There is a risk that errors could occur in the calculation and entry of direct debit amounts and incorrect rents are collected from tenants. This could result in tenant dissatisfaction, adverse publicity and significant remedial work to resolve the situation.	to reduce manual processing for calculation and input of direct debit values. Consideration should be given to using spreadsheets to export rent amounts and frequency of direct debit payment and use formulae to calculate the direct debit amount. The Council should liaise with Civica to explore the potential for this data to be imported to the Saffron system. We also recommend that, once all changes are processed, there is independent verification of the direct debit calculations to confirm their accuracy. Grade 3		rent over 47 weeks if tenants have arrears of rent their payments are calculated over 52 weeks. We do not agree that the exporting or importing of rent or direct debit figures would satisfy our business requirements. We will use a formula to calculate the Direct Debit payment, retain the calculation and have this independently calculated. **To be actioned by:** Marion Smith, Section Head Revenue & Benefits **No later than:** 30th September 2011		
	7.3 Error Correction and Validation Our review noted that error reports for processing data were produced automatically. For example, rejected BACS payments reports are dealt with by	We recommend that all forms detailing corrective action are signed by the		We will ensure this recommendation is		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	the Rents team. We noted that forms are completed to support any adjustments made within the system; however, our review found that the forms are not completed correctly or signed as having been independently checked. There is a risk that amendments to data within the system are made without appropriate authorisation.	user's line manager. We also recommend that the forms are completed in their entirety to clarify the source of the amendment. Grade 3		actioned. **To be actioned by:** Marion Smith, Section Head Revenues & Benefits **No later than:** Immediate		
	8.1 Continuity Planning During the course of our discussions with staff, we noted that there are no formal business continuity plans in place that could be invoked in the event of a disaster. As an example, within Rents, reliance is	We recommend that management ensure business continuity plans are		**Rent Accounting** A business continuity plan will be developed		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	placed on ICT to restore Saffron quickly. There are no plans to deal with any long-term loss of systems. The absence of business continuity plans increases the risk that the Council will be unable to respond effectively to a disaster, affecting services and leading to adverse publicity.	developed for all areas reliant on the Saffron system. The plans should consider all scenarios which could impact on the ability of the department to perform their role. For example, loss of access to offices, loss of system access etc. We also recommend that once the plans are developed, management ensure they are subject to regular testing to confirm that they support the response to a disaster. Grade 4		for the rent accounting module in Saffron. **To be actioned by:** Marion Smith, Section Head Revenue & Benefits **No later than:** 31st March 2012 **Housing** A Business Continuity Plan will be developed for both repairs and homelessness modules. **To be action by:** Janice Lockhart, Homelessness and Allocations Manager & Stephen McGonagle, Maintenance & Repairs Manager **No later than:** 31st March 2012		
	8.2 Disaster Recovery We noted that the last full disaster recovery exercise had been carried out in 2007, before the migration to Saffron v6. Real-time disasters, such as a power outage, have occurred since then, from which the Council has been able to restore services within a	We recommend that formal plans are developed by ICT which detail the processes to be followed in the event of		Agreed **To be actioned by**: Iain Kerr, ICT Security		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	reasonable time. ICT is currently formulating a new Disaster Recovery Plan for all systems within its remit. This involves a new facility in Clydebank which is being developed in conjunction with NVT Computing. However, until this work is complete there is no disaster recovery plan in place for the Saffron system. There is a risk that the lack of a plan to address immediate disasters could result in delays in restoring the Saffron system in a timely manner.	a disaster impacting on the availability of the Saffron system. We recommend that ICT management liaise with HEED management to determine the restart priority of the system. This should reflect the timing of the disaster recovery process e.g. month end, direct debit processing timetables etc. We also recommend that the Disaster Recovery plan is tested at regular intervals to confirm that the plan supports ICT's response to a disaster. Grade 4		Officer **No later than:** 31st March 2012 ICT will review restart priority with Departments **To be actioned by:** Iain Kerr, ICT Security Officer **No later than:** 31st September 2011 Agree that Disaster Recovery plan should be tested. However, currently live restores are performed for Saffron system providing reassurance that delays are not being experienced. **To be actioned by:** Iain Kerr, ICT Security Officer **No later than:** 31st March 2012		
	8.3 Backup Media System data is backed up on a nightly basis and the operating system and application is backed up weekly and monthly. We were pleased to note that there is a policy of retaining these tapes in an off-site	We recommend that management ensure that they devise a schedule for testing the restoration of data and the operating system from backup media.		Full Saffron restore of application and operating system onto an independent hardware platform to be scheduled.		

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff) **Date Issued : March 2011**					**Action Plan 3**	
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	location. While recognising that the data files have been restored on an ad-hoc basis from backup media, we noted that there was no formal process in place to test backup media to confirm that data and the operating system can be recovered. There is a risk that by not performing regular test restores of data and operating systems from backup media, assurance cannot be gained that backup media can be relied upon for restoring the system in the event of a disaster. This could result in partial or total loss of system data.	This will provide assurance that backup media can be relied upon in the event of a disaster. Grade 3		The full Saffron restore exercise and any future restores will be logged in the log to provide assurance and a record of the actions taken. Full Saffron system test restores will be incorporated into a restore timetable according to priority and urgency with the other corporate ICT applications. **To be actioned by:** John Martin, Section Leader ICT Connect **No later than:** 31st August 2011		
	9.1 Audit Logs During our discussions with staff, we noted that staff were generally unaware of audit logs within Saffron. At the time of our audit, staff had to contact the software supplier to determine whether any logs were present within the system. The supplier responded to indicate where audit logs can be	We recommend that audit logs are reviewed on a regular basis. This would give assurance that access to the system is appropriate. It would also afford the opportunity to identify any		Agreed. ICT will switch on Audit feature and review / risk assess performance. Approach vendor to determine if there's an associated cost. Review of the logs to assess if unauthorised or inappropriate access to data		

Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	located within the system and what is recorded. We noted that a number of the audit logs had been deactivated on the basis that they were affecting system performance. In addition, we noted that there is no monitoring of direct access to the Saffron database by ICT staff. There is a risk that the lack of use of audit logs undermines the security around Saffron, potentially allowing unauthorised access to go undetected. There is also a risk that performance-affecting issues are not identified and resolved. There is also a risk that inappropriate direct access to the database is not detected.	performance issues within the system which could be raised with Civica. Consideration should be given to archiving larger logs to avoid any detrimental effect on the system, whilst retaining an appropriate audit trail. Grade 4		would require to be assessed by HEED. **To be actioned by:** Brian Miller, Section Leader ICT Infrastructure **No later than:** 31st December 2011		
11.1 Server Room Security During our review, we noted that access to the server room is controlled by a numeric keypad. The keypad is dated and has five numeric buttons, restricting the range of combinations which can be set. We noted that the access code had not been changed for at least three years and that the same	We recommend that management improve access controls to the server room. This should ensure that all access to the room can be attributed to an individual. Consideration should be given to extending the use of the system		ICT Security Officer will review this procedure and engage with Health & Safety for advice.		

Ref. No.	Finding	Recommendation	Priority	Management Comment	Manager Responsible	Date of Action
	code is used by all personnel. We also noted that a book is maintained to record access to the server room. However, completion of this cannot be enforced. There is a risk that, by not changing the keypad code, former employees may be able to gain access to the room. In addition, there is an increased risk of the code becoming known to unauthorised personnel. There is also a risk that ICT is unable to determine those parties who have accessed the server room and the purpose for this visit.	in place within the Council Headquarters. If this is to be used ICT should ensure that they have sole responsibility for controlling access to the server room. Grade 3		**To be actioned by:** Iain Kerr, ICT Security Officer **No later than:** 31st December 2011		
	11.2 Server Room Environment We observed that the server room temperature is controlled by four air conditioning units. Discussions revealed that two of the air conditioning units are back-ups in the event of the other units failing. The units are sized so that they do not run at full capacity. However, we noted that there is no mechanism to remotely monitor temperatures or to receive alerts	We recommend that management consider the implementation of a system which supports remote monitoring of the temperature in the server room. This should either aim to provide details of the temperature via a console that can be accessed remotely or, preferably, through a system which sends SMS/text alerts to ICT personnel when		A capital bid has been approved for improvements to environmental controls. **To be actioned by:** Brian Miller, Section		

Systems Review Action Plan: - Saffron System Audit (Scott Moncrieff)						**Action Plan 3**
Date Issued : March 2011						
Ref. No.	**Finding**	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date of Action**
	when temperatures exceed tolerance levels in the server room. There is a risk that ICT staff would not be alerted to excessive temperatures in the server room. This could result in failure of key network devices and disruption to network and system availability.	temperatures exceed agreed tolerances. Grade 3		Leader ICT Infrastructure **No later than:** 30th November 2011		