

2008-09 ACTION PLAN – ICT SERVICES			Receiving Officers: DP/ CJP / ICT Managers			
			Responsible for Reply: Chris Powell			
Audit Officer – Graham Stubbs – Contract Computer Auditor			FOLLOW UP SECTION			
	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
4.1 Management Controls						
C U R R E N T R I S K	4.1.1 Compliance with Policies					
	4.1.1.1 Email Policy Further research should be conducted to establish whether just sending a link as opposed to attaching the text itself creates any issues.	C J Powell (January 2009)	Will consult Legal services	4.1.1.1 Legal services asked for advice on 24/8/09 and now awaiting results of research. Results: Best practice, in legal terms, is to put the disclaimer at the front of every email. This is not a popular action as it make the email more difficult to read and few councils do this. Putting the disclaimer in a link at the end of each email does cover us and does make the email more readable.		R E S I D U A L R I S K
	4.1.1.2 Email Policy Breaches Internal Audit should be fully informed when any instances of non compliance with the Email Policy occur. The ownership of the Email Policy should be investigated and the policy and processes changed as appropriate	C J Powell (March 2009)	Agreed	4.1.1.2 Agreed. A single swear word constitutes a breach of the email policy and the automatic scanners pick this up. This occurs mainly with incoming emails over which we have no control. In the interests of efficiency and pragmatism these single instances are not raised to management or audit. Breaches of policy that are more significant are reported to audit (and the Programme Board) who will convene the Fraud Forum as they see fit. Ownership reviewed and remains as is. Owned by HR with support from ICT and Legal.		
	4.1.1.3 Security Breaches Internal Audit should be fully informed when any security breaches occur.	C J Powell (March 2009)	Agreed	4.1.1.3 Agreed as per 4.1.1.2	Green	
Yellow						

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.1 Management Controls					
C U R R E N T R I S K	<p>4.1.2 Contract Staff Policy Compliance All contract staff should be fully registered in the Trent system and included in the total headcount figures presented to council members.</p> <p>Interflex Contract staff should be made to clock in and out along with the majority of council staff.</p> <p>Legal Compliance If the ICT service intend to continue to use Synergykey then this company should be added to the council's 'preferred supplier' list, which we understand is now controlled by Devon County Council.</p>	<p>Agreed Audit Contractor (GS) January 2009</p> <p>C J Powell / T Wilson (March 2009)</p> <p>C J Powell / K Jenkins (March 2009)</p>	<p>The Head of ICT stated that he sent the necessary paperwork to HR.</p> <p>An audit of HR/Payroll will be commenced in January 2009 and this will be verified during the review.</p>	<p>The policy of clocking in of "contract" staff is with payroll to determine. Temps, contract staff, contractors and consultants will all then follow this policy.</p> <p>The DCC preferred suppliers list will be investigated and Synergykey will be added if possible.</p> <p>In progress aiming for March 2010.</p>		R E S I D U A L R I S K
	Yellow				Green	

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.1 Management Controls					
C U R R E N T R I S K	<p>4.1.3 Reporting to the Programme Board The end project reports submitted to the Programme Board should show:</p> <ul style="list-style-type: none"> • The original cost estimate from the Business Case • The eventual cost • The original 'planned' start date 'v' the actual start date <p>The incorporation of the above would allow the Programme Board to be more 'challenging' of the information presented. For instance, the Novell-Microsoft migration had a cost estimate of £47,000 in the business case, an agreed Budget of £50,000 and total cost to date of £157,509 as at (October 2008).</p> <p>We are also of the opinion that this cost will rise further.</p> <p>Yellow</p>	C J Powell (March 2009)	<p>Changes will be made to the information presented to the Programme Board</p> <p>Miscoding in Cedar will be corrected.</p>	<p>The presentation of information for the Programme Board is continually evolving as needs arise.</p> <p>Changes to the presentation have been made recently to provide direct connection to the Finance System.</p> <p>The miscodings in Cedar were corrected in January.</p> <p>The project costs have not risen further since the recoding.</p>	Green	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.1 Management Controls					
C U R R E N T R I S K	<p>4.1.3 Reporting to the Programme Board Continued ...</p> <p>The information provided to the Programme Board should contain additional information in line with the above points to enable a more 'challenging' response.</p> <p>In line with other officer groups in the council, consideration should be given to extending the membership of the Programme Board to ensure more objectivity and independence; for instance the Portfolio Holder for ICT could be invited.</p> <p>Internal Audit will investigate the subject of budget entry in their review of the main accountancy system due to take place in early 2009.</p> <p>Yellow</p>	<p>C J Powell (March 2009)</p> <p>Disagree C J Powell</p> <p>Internal Audit (Jan 2009)</p>	<p>Changes will be made to the information presented to the Programme Board</p> <p>The Portfolio Holder receives copies of Programme Board minutes</p>	<p>As from previous answer the information and presentation will continuously evolve.</p> <p>The Portfolio holder continues to receive copies of the minutes.</p>	<p>Green</p>	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.1 Management Controls					
C U R R E N T R I S K	<p>4.1.6 Control of Contractors</p> <p>All contractors must be registered in Trent and expiry dates should be set for say 6 months to enable more effective monitoring and statutory reporting of the total council headcount.</p>	<p>Agreed Audit Contractor (GS) January 2009</p>	<p>An audit of HR/Payroll will be commenced in January 2009 and this will be confirmed during the review.</p>			R E S I D U A L R I S K
	Yellow				Green	

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.1 Management Controls					
C U R R E N T R I S K	<p>4.1.7 Microsoft Migration / Office 2007 A mechanism exists within CSOs to draw up a preferred list of contractors/suppliers to carry out work for the council.</p> <p>In future, the Corporate Director should ensure that a public advertisement is placed in the local newspaper and on the council's web site seeking expressions of interest from ICT service companies/contractors located in Devon.</p> <p>Arising from this exercise the Corporate Director should ensure the production of a select list of preferred contractors/suppliers and ensure that this list is maintained by an independent directorate/sub-directorate.</p> <p>Any further quotation exercises should utilise the companies/contractors appearing on the councils preferred list.</p> <p>Red</p>	<p>C J Powell December 2008</p>	<p>CSO to be followed when awarding contracts for the supply of goods and services.</p> <p>Exemption to CSO to be applied for in accordance with the established procedure (if applicable).</p>	<p>The exemption to CSO process will be used appropriately.</p> <p>The new Procurement Officer will be approached to investigate adding suppliers to the Council's "preferred supplier" list.</p>	<p>Green</p>	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementatio n date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implement ation	
	4.2 Access Controls					
C U R R E N T R I S K	<p>4.2.1 Compliance with ICT Security Policy</p> <p>The agreed action from the previous report should be complied with.</p> <p>4.2.2 Leavers</p> <p>Tighter control should be exercised over staff leavers to ensure that email addresses are removed as soon as possible.</p> <p>The anomalies highlighted above should be investigated and remedial action taken as appropriate.</p> <p>Yellow</p>	<p>C J Powell (December 2008)</p> <p>C J Powell (March 2009)</p> <p>C J Powell (March 2009)</p>	<p>Improved Leavers procedures will be discussed with HR.</p>	<p>4.2.1</p> <p>Obtaining and maintaining appropriate security conditions is an ever-changing battle. In an effort to achieve some sort of commonality amongst councils the government has set the CESG (the government information security organisation linked to GSHQ) to develop a Code of Compliance (known as CoCo). These 90 wide-ranging security controls now have to be met in order for the Council to be allowed to use the secure connection to the secure government intranet, the GSx, which is currently providing access to DWP systems.</p> <p>We had made sufficient progress in achieving these 90 controls that the Council gained CoCo in March 2009. We are still working to complete the committed actions.</p> <p>We will have to go through this check every year from now on with the standards and the controls changing every time.</p> <p>4.2.2 Leavers</p> <p>The leavers process relies initially upon the relevant manager informing ICT that staff are leaving and, as a back-stop, a leavers report run from the HR system when their payroll finishes. Once logged onto the ICT Helpdesk there is a set action list, including sending an email to the manager of the leaver asking them if there is anything they need to do with the leaver's email messages or settings before the account is closed. Sometimes they request that it is left open for a</p>	<p>Green</p>	R E S I D U A L R I S K

Yellow				<p>time while contacts are dealt with.</p> <p>The process is being reviewed to see if these few exceptions can be managed more robustly rather than relying upon the business manager to inform ICT when the work has finished.</p> <p>Target date march 2010</p>	Green	
--------	--	--	--	---	-------	--

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.2 Access Controls					
C U R R E N T R I S K	<p>4.2.3 Active Directory User List</p> <p>The anomalies highlighted should be investigated and appropriate remedial action taken.</p> <p>Periodic reconciliation exercises should be performed.</p> <p>4.2.4 Penetration Testing</p> <p>Confirmation should be received that these issues are being addressed</p>	<p>C J Powell (March 2009)</p> <p>C J Powell (March 2009)</p> <p>C J Powell (March 2009)</p>	<p>Still an active project</p>	<p>4.2.3 User list</p> <p>The work to complete the Microsoft migration is progressing but the initial user reconciliation of the new AD environment has been completed.</p> <p>The update process is being automated in September.</p> <p>A further reconciliation exercise is intended for Feb 2010 once all the servers have been migrated.</p> <p>4.2.4 Pen Testing</p> <p>A major requirement of CoCo, the Council now has in place a contract for a security company to carry out quarterly penetration testing of all of our public internet addresses.</p> <p>Also, a new internal security monitoring system runs monthly to check the risk status of the internal servers and PCs.</p> <p>Actions plans from these tests are now run by the Design and Compliance Team.</p>	Green	R E S I D U A L R I S K
	Yellow					

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.2 Access Controls					
C U R R E N T R I S K	<p>4.2.5 Privileged Accounts</p> <p>The problems highlighted should be investigated and remedial action taken as appropriate.</p> <p>System logs relating to the activity of domain administrator accounts assigned to external suppliers will be checked daily and activities analysed</p> <p>4.2.6 Software Updating and Patching</p> <p>A uniform approach to patching of system software should exist and the user's ability to change any system setting which would affect this should be disabled.</p> <p>Use should be made of Security Analysis software to check servers and PC's for incorrect levels of system software patching and any open 'shares' which may have come into being.</p> <p>Yellow</p>	<p>C J Powell End March 2009</p> <p>C J Powell End March 2009</p> <p>C J Powell End March 2009</p> <p>C J Powell End March 2009</p>	<p>Security related issues will be addressed as part of the end-project security review and CoCo compliance</p> <p>Security related issues will be addressed as part of the end-project security review and CoCo compliance</p> <p>Security related issues will be addressed as part of the end-project security review and CoCo compliance.</p>	<p>4.2.5 A review of all users accounts has been carried out as part of the Microsoft migration. Server accounts will be examined as each application and machine is migrated.</p> <p>System logs are proving too unwieldy to determine information and so a small control system is being sought to translate the logs into "English". This is in test and looking for a go-live by March 2010.</p> <p>4.2.6 The Microsoft migration has included the design of a "lock-down" desktop that prevents users from altering most of the critical settings.</p> <p>Patching policies and systems have been produced and all PCs are subject to this. Server policy has been introduced and the final changes will be made once the last server is migrated into the new Microsoft domain, around Dec 2009.</p>	Green	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.2 Access Controls					
C U R R E N T R I S K	<p>4.2.7 Network Security Weaknesses</p> <p>Where possible the ability of the 'Everyone' Group to have access to information should be disabled.</p> <p>Sensitive data on the servers should be restricted to groups of users who have the need to access the data as part of their job function.</p> <p>4.2.8 Windows XP Security Weaknesses</p> <p>The above weaknesses in PC setup should be rectified by use of Access Control Lists and other measures to prevent non-administrative users having access to Windows XP features which are not job related</p> <p>Red</p>	<p>C J Powell End March 2009</p> <p>C J Powell End March 2009</p> <p>C J Powell End March 2009</p>	<p>Security related issues will be addressed as part of the end-project security review and CoCo compliance</p> <p>Security related issues will be addressed as part of the end-project security review and CoCo compliance</p>	<p>4.2.7</p> <p>The "everyone" group was a problem that appeared on initial migration and was quickly resolved in most areas. User access to systems and access to was reviewed and risks identified. Of the 91 shares identified one significant issue remains and that is with the AIMS system. This is being dealt with in three ways:</p> <ul style="list-style-type: none"> - Reducing the number of users from over 100 to around 12 through implementation of a replacement credit card payment system - Continued pressure on the supplier to amend their product - Working carefully through the software on a trial and error basis to determine what minimum access rights will work <p>The data access policy is one of "least privilege" as required by CoCo and this is set up a part of normal business.</p>	<p>Green</p>	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.3 Operational Controls					
C U R R E N T R I S K	<p>4.3.3 Incident and Problem Management</p> <p>A more formal process for problem management should be introduced and visible reporting of downtime and problems should be made available to the wider user community with the Intranet being a possible vehicle.</p> <p>Heads of Service should be reminded that all support calls to external suppliers should be routed through the Helpdesk.</p> <p>Internal Audit will investigate problem management in more depth during the next review.</p> <p>4.3.4 ICT Asset Disposal</p> <p>The Asset Disposal Policy (currently being written by Internal Audit) should be revised to address the need for additional measures in respect of ICT equipment.</p> <p>Yellow</p>	<p>C J Powell (July 2009)</p> <p>C J Powell (January 2009)</p> <p>Internal Audit (March 2009)</p>	<p>Will be included in the Intranet redesign.</p> <p>Draft Disposal Policy, Strategy and affiliated appendices has been completed and is being consulted on by HoS and SMT.</p>	<p>The IMPACT process that has been running for two years and analyses the root cause of problems and looks for solutions.</p> <p>The information produced by the analysis will be made transparent once the new intranet is launched by Feb 2010.</p> <p>4.3.4 ICT have been running an asset disposal process for two years and this process appears to be working.</p>	<p>Green</p>	R E S I D U A L R I S K

	Actions agreed by Corporate Director and Head of ICT	Implementation date and officer responsible	Auditor Notes	Head of Service Confirmation of compliance	Actual Date of Implementation	
	4.4 Systems Development					
C U R R E N T R I S K	<p>4.4.1 Monitoring of Projects</p> <p>The integrity of the spreadsheet used to create the Programme Board report should be investigated.</p>	C J Powell (December 2008)	A bug in the spreadsheet has been corrected.	<p>4.4.1</p> <p>The programme board report will continue to evolve as different information is required by the directors and other users of the report.</p>		R E S I D U A L R I S K
	Yellow				Green	