

## INTERNAL AUDIT REPORTS FINALISED LATE MARCH 2010

### Final audit reports issued:

<b>Audit Title:</b>	<b>Crime and Disorder</b>			<b>Date of Audit:</b>	November – December 2009		
<b>Number of High Priority Recommendations:</b>	0	<b>Current Audit Opinion:</b>	2	<b>Previous Audit Opinion:</b>	N/A	<b>Overall Evaluation (Risk):</b>	<b>Moderate</b>
<b><u>Key Findings and Recommendations</u></b>							
<p>Our review examined whether arrangements for developing, financing and initiating arrangements to counter crime and disorder are robust and efficient. No high priority recommendations were made following the review. However, the following medium priority recommendations were made:</p> <ul style="list-style-type: none"><li>• Benchmarking of performance indicators against other Community Safety Partnerships (CSP's) should be developed further. This would put Swindon's performance in context and also allow the Annual Strategic Assessment to be better informed.</li><li>• A timescale and project plan should be put in place to complete and roll out the Outcome Framework to assist in interpreting performance indicators and, again, further inform the Annual Strategic Assessment.</li><li>• A risk register should be maintained and kept under review for the CSP's delivery of local and national priorities. The risk register should be included as a standing item on the agendas of the Executive Board and Joint Commissioning Board.</li><li>• Future CSP Strategic Assessments should reflect the Council's Connecting People, Connecting Places initiative and community views so that the CSP's aims can be put into practice in ways that meet the expressed needs of local communities.</li></ul>							

Audit Title:	LAA Grant Claim				Date of Audit:		January 2010	
Number of High Priority Recommendations:	N/A	Current Audit Opinion:	N/A	Previous Audit Opinion:	N/A	Overall Evaluation (Risk):	No overall opinion	
<u>Key Findings and Recommendations</u>								
A certification audit was carried out on the Council’s LAA grant claim.								

## INTERNAL AUDIT REPORTS FINALISED LATE MARCH 2010

<b>Audit Title:</b>	<b>St Catherine's</b>		<b>Date of Audit:</b>	January 2010	
<b>Current Audit Opinion:</b>	2	<b>Previous Audit Opinion:</b>	N/A	<b>Overall Evaluation (Risk):</b>	<b>Moderate</b>
<b><u>Key Findings and Recommendations</u></b>					
<p>St Catherine's School was externally assessed by Internal Audit against the DfES Financial Management Standard in Schools (FMSiS) and was given a conditional pass.</p> <p>An audit of the school was also completed resulting in an overall opinion of 'satisfactory'. Recommendations have been made and agreed to ensure that all weaknesses identified are addressed.</p>					

<b>Audit Title:</b>	<b>Disciplinary Investigation/Hearing (WB 09/10-7)</b>			<b>Date of Audit:</b>	March 2010	
<b>Current Audit Opinion:</b>	N/A	<b>Previous Audit Opinion:</b>	N/A	<b>Overall Evaluation (Risk):</b>	N/A	
<b><u>Key Findings and Recommendations</u></b>						
Internal Audit conducted an investigation in to allegations relating to improper recruitment. The case went to a disciplinary hearing where the employee received n informal reprimand.						

## INTERNAL AUDIT REPORTS FINALISED LATE MARCH 2010

<b>Audit Title:</b>	<b>Creditors</b>		<b>Date of Audit:</b>	March 2010	
<b>Current Audit Opinion:</b>	3	<b>Previous Audit Opinion:</b>	3	<b>Overall Evaluation (Risk):</b>	<b>Of Concern</b>
<b><u>Key Findings and Recommendations</u></b> <p>The key recommendations made as a result of the review are:</p> <ul style="list-style-type: none"> <li>• As agreed, the Continuous Service Improvement Plan (CSIP) will extend to provide for the implementation of audit recommendations. To achieve this there must be a clear link between individual audit report action plan points and the CSIP. This should enable all audit recommendations to be implemented by the agreed dates.</li> <li>• In accordance with Financial Regulations, official orders should be produced to provide an approved financial commitment i.e. prior to the receipt of invoices for works, services or supplies. There should also be a segregation of duties and independent check at the order, delivery and payment stage. Also, invoices should not be processed for payment without the full completion of both the authorisation and certification of payment grids.</li> <li>• Supplier information should only be entered onto the Oracle Financials Accounts Payable System upon receipt/completion of a supplier setup/amendment form. Before a new suppliers is set up careful scrutiny of existing suppliers should be undertaken to minimise possible duplication of suppliers on the system.</li> <li>• The payment authorised signatory list should be updated on a timely basis in respect of the leaver's lists received on a monthly basis. The authorised signatory listing is not currently up to date and requires a full review to ensure that all information is still relevant. The authorised signatory list should be checked prior to the payment of invoices to ensure that the invoice signatory limits are appropriate.</li> <li>• A review of duplicate payments and credit notes should be undertaken on a periodic basis to ensure that any monies that are owed to the Council are recovered in a timely manner. There are standard reports in relation to both duplicate payments and credit notes that can be produced from the Oracle Financial Accounts Payable System and these should be run and reviewed.</li> </ul>					

## INTERNAL AUDIT REPORTS FINALISED LATE MARCH 2010

<b>Audit Title:</b>	<b>Risk Management</b>		<b>Date of Audit:</b>	March 2010	
<b>Current Audit Opinion:</b>	3	<b>Previous Audit Opinion:</b>	3	<b>Overall Evaluation (Risk):</b>	<b>Of Concern</b>
<b><u>Key Findings and Recommendations</u></b> <p>The key recommendations made as a result of the review are:</p> <ul style="list-style-type: none"> <li>• A common approach to managing risks is in place however this is not consistently followed. A quality assurance role process should be implemented to ensure that all service areas produce risk registers on a timely basis and follow risk management guidance to achieve consistency and required standards.</li> <li>• Following the restructuring of the corporate risk and performance functions under the Head of Performance and Risk, the supporting structure and role of risk and performance champions should also be reviewed. This will ensure that that performance is aligned and linked to individual risks as an aid to risk monitoring. The risk strategy makes reference to performance management, but this may need to be reviewed in light of changes regarding the role of risk and performance champions.</li> <li>• In accordance with the risk strategy, roles and responsibilities, the Corporate Risk Management Group meetings should be recommenced without delay and thereafter held quarterly as per the terms and conditions of the group. In the event that these meetings are not held quarterly, Corporate Board and Audit Committee should be advised (as per the communication structure set out in the strategy) and action taken where appropriate.</li> <li>• The reporting structure for risk management should be reviewed to include full reporting at all levels i.e. department, directorate, group directorate and corporate. Risk and performance champions should be identified at operational levels of the Council and tasked in assisting with embedding risk management across the Council. Responsibility should also be assigned for the completion of risk registers and the risk management process within the Directorates.</li> <li>• The PCT partnership risk registers and reporting process should be reviewed as a matter of urgency to ensure that risks are appropriately considered prior to decision-making.</li> <li>• A central repository for performance and risk should be made available in order to present up to date information, particularly for risk registers, as this will also improve the efficiency of monitoring processes.</li> <li>• An Information Security Forum has been set up as recommended in the last audit. However, the group is not performing its role of evaluating information technology risks faced by the Council, as meetings have not taken place.</li> </ul> <p>A full copy of the report is included with this evening's agenda item: Risk Management Update.</p>					

## INTERNAL AUDIT REPORTS FINALISED LATE MARCH 2010

<b>Audit Title:</b>	<b>Lydiard House</b>		<b>Date of Audit:</b>	March 2010	
<b>Current Audit Opinion:</b>	3	<b>Previous Audit Opinion:</b>	3	<b>Overall Evaluation (Risk):</b>	<b>Moderate</b>

### **Key Findings and Recommendations**

The key recommendations made as a result of the review are:

- The PDQ machine at Lydiard House does not comply with the Payment Card Industry Data Security Standards (PCIDSS). At present the full customer credit/debit card number is printed on both the customer and office copy, instead of just the last 4 digits as required by the standard. Without further delay and to comply with the PCIDSS a compliant PDQ machine should be installed. Office copy receipts held on site should be shredded to ensure compliance with the Data Protection Act and to mitigate the risk of identity theft.
- In compliance with Financial Regulations official orders should be raised at the point of commitment with relevant checks completed at the certification of payment stage, including that an appropriate number of quotations have been sought for procurement of goods/services.
- Reconciliation of the budget monitoring spreadsheet should be undertaken to ensure accuracy in financial reporting and care should be taken to avoid transposition errors occurring.
- All petty cash slips must be approved for payment and signed by the recipient on reimbursement.
- Lydiard House must provide effective and timely calculation and recharging of electricity usage by Chartridge Conference Limited for the on site conference centre. This is to ensure that the basis of electricity recharging is followed as set out in the lease agreement and to address previous undercharging and inappropriate treatment of VAT.
- A Lydiard House risk register should be introduced and maintained. Where necessary this should be linked with departmental and group risk registers in the event of high impact/materiality risks that require escalation.
- A full review of the Clarity system with regards to access and the issuing of clarity cards to ensure people do not share cards and that the level of access is appropriate to their job.
- The introduction of new CCTV equipment to the outside of Lydiard House giving increased security.
- The introduction of procedures for the CCTV system including the logging of back-up discs and the safe storage of this data at an off-site location.