Audit Committee 13 March 2012

Internal audit – Review of recommendations

Executive summary and recommendations

At its meeting on 29 September 2011, the Committee agreed that it should receive a paper at each meeting, setting out progress on recommendations from internal audit reports.

Most of the information in the appendix is taken from the wording of the internal audit reports. The exception is the "update" section in the right-hand column, which provides details of progress.

Decision

The Committee is requested to discuss the paper.

Background information

Please refer to individual internal audit reports for the background to recommendations.

Resource implications

None

Financial implications

None

Appendices

None

Date of paper

8 February 2012

Date	Ver.	Dept/Cmte	Doc Type	Title	Status	Int. Aud.
2011-10-03	a	AUD	PPR	Executive summary review of recommendations Audit Committee 13 March 2012	Final DD: None	Public RD: None

Recommendations from internal audit reports 2011-12

Information Security/Data protection (report dated September 2011 – considered at Audit Committee 29 September 2011)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	**Number of recommendations**
Fundamental	None
Significant	None
Housekeeping	9

Risk 1: Electronic data is removed inappropriately by an employee (Data Security – Risk No 17.1)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/responsibility**
1	*Observation:* Staff are asked to sign up to the Information Technology Policy under section 5h of the Employee Handbook. This policy details the responsibilities of the staff and the use of devices such as laptops and PDA's and use of email, telephone calls etc. Whilst it mentions that information held on USB drives is the property of HPC, it does not mention HPC's specific policy in respect of these tools. For example, the responsibilities of Staff using USB drives, that only encrypted drives can	As planned, HPC should review and update the Information Technology Policy held within the Employee Handbook to ensure it provides more detail on the use of USB data drives.	Housekeeping	A review of the IT Policy is scheduled for 2012-13 financial year. These updates will reflect changes in technology that are rolled out to the organisation over the next few months	2012-13 Financial year Director of HR /Director of IT

	be used, what USBs should be used for and the security of these. We were informed that the Policy is currently being reviewed and should be in place from September 2011. *Risk:* Staff are not fully aware of their responsibilities in respect of the use of USB data drives.				
2	*Observation:* A report was provided by the Head of Business Process Improvement which detailed a review of the Payment Card Industry (PCI) process. One of the weaknesses identified was where data was taken over the telephone, it was not secure enough to ensure personal data could not be copied. There were also concerns over the security of the PDQ machine for walk in applicants and the arrangements around the collecting of the Section 10 on the International Application Forms which contain credit card details. HPC is investing in Semafone in September 2011 which will provide an automatic third party process which will	HPC should continue to address the issues identified in the recent PCI report.	Housekeeping	This project is in progress, and is currently awaiting action by utilities to transfer specific telephone numbers to new services.	End of year Director of Finance **Update:** Preparation work for implementation continues. The project is due to be implemented in February 2012.

	remove any staff needing to take responsibility for taking credit card details. The PDQ machine is also going to be moved into a more secure area, and Section 10 details will be held more securely in the interim, but it is intended that this transaction will be dealt with by Semafone also. *Risk:* Loss of bank and credit card details.				
3	*Observation:* Through discussion with the HR Manager, the Director of Operations and the Head of Business Process Improvement there tended to be a view that HPC did not have a formal leavers checklist in place which ensured that all issued items, such as Blackberry's , ID cards, etc were returned and all appropriate departments such as IT, Payroll, etc were informed in a timely manner. At the debrief, this was questioned by the Chief Executive and a copy of a checklist was provided which covered most key areas, though it was felt it would benefit from a more formal list of all potential items that should be returned to ensure that nothing could be missed off.	The HR team should review and update the Leaver's checklist to ensure that it covers off all key areas and items that need returning. Once reviewed this should be communicated to managers across the organisation so that they are fully aware of the checklist.	Housekeeping.	The list will be reviewed and updated where required. The list will be circulated to all EMT, CDT and line managers.	November 2011 Director of HR / HR Manager **Update:** A new on-line leavers form, including an updated checklist for managers has been introduced and is now in use across the organisation.

	Risk: Failure to ensure that Leavers do not take away items which contain personal information.				

Risk 2: Paper record Data Security (Data Security – Risk No 17.2).

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
4	*Observation:* Locked document destruction bins were observed as being in place within each department visited. A bag is suspended in each of the bins and confidential documentation is placed in the locked bins and emptied on a weekly basis by Iron Mountain. The service level agreement with Iron Mountain specifies the responsibilities of both parties. It was noted however that this states that HPC staff are responsible for the tying up and sealing of the bags, but having spoken with staff this part of the process is performed by Iron Mountain. At the time of the audit we did not witness the Iron Mountain process in practice. *Risk:* Confusion over the responsibilities of both parties in the agreement, which could be problematic in the event of any data security arising.	HPC should revisit the service level agreement with Iron Mountain and ensure this is updated to reflect current roles and responsibilities in respect of tying and sealing of the bags.	Housekeeping	The current method of collection used by Iron Mountain utilises a large blue "wheelie bin" transported around the office buildings to each location, where the bins contents are emptied directly into the blue bin. Bag securing is no longer required. The Facilities Manager will attempt to have the SLA updated, although it is believed to be generic across all clients, and resistance may be incurred.	December 2011 Facilities Manager

5	*Observation:* The Director for Fitness to Practise provided us with a document retention policy which is used within their team and clearly sets out the timescales for retaining different documents. HPC also has a Destruction (and Retention) Policy which was created in 2005, when the Freedom of Information Act came into force. Whilst it provides a high level list of documents held and retention dates it has been accepted by management that there is a need to develop a more comprehensive retention policy on a similar line to the Fitness to Practise document. *Risk:* Failure to comply with the Data Protection Act by keeping personal information beyond timescales which the Act deems appropriate.	As planned HPC should look to expanding and enhancing their current Destruction (and Retention) Policy to match the style of the document retention policy in place with Fitness to Practise. Once completed this policy should be agreed with all departments and then communicated to all parties. In addition, consideration for encompassing the FTP document already in existence into this document.	Housekeeping	A high level organisation wide destruction / retention table has existed since 2005 A scheduled updating of policies will produce a document similar to the FTP Retention policy. Individual departments are aware of the retention requirements relating to their own areas.	Next 6 months Director of Operations

6	*Observation:* Section 8a of the Employee handbook provides explicit detail on the Office Security Policy. Whilst it contains a summary of some of the key measures such as locking all room, not divulging access codes etc., it did not include ensuring that sensitive information is securely locked in cabinets when the office is unmanned. It was also noted that there is currently no 'clear desk policy' in place. *Risk:* Loss of personal data due to failure to ensure effective office security processes in place.	HPC should consider updating the Office Security Policy within the Employee Handbook to make explicit reference to ensuring that all filing cabinets are locked when the section is unmanned. When practical the organisation should look towards introducing a 'clear desk policy' to ensure that all sensitive and personal data is locked away at the end of each day. Once implemented this should be detailed in the Employee Handbook.	Housekeeping Housekeeping	Departmental guidelines require confidential material to be secured overnight, however we will look to update the employee handbook	By April 2012 Head of BPI & Facilities Manager (Director of HR)

7	*Observation:* The Employee Handbook includes a section on crime and data protection. In review of this we noted that it did not explicitly explain the importance of data protection to staff, nor detail the responsibilities of the Council or staff in respect of use of and security over personal data. The Secretary to the Council later provided us with the Freedom of Information/Data Protection HPC Policy and Procedure which gave a brief guide on data protection and subject access requests. *Risk:* Misleading or inadequate information detailed within the Employee Handbook on data protection.	Consideration be given to including the Freedom of Information/Data Protection HPC Policy and Procedure document within the Employee Handbook to ensure that staff are fully aware of the responsibilities regarding data protection and the process for subject data access.	Housekeeping	The current handbook content will be reviewed and ensure it matches other more detailed guidance elsewhere.	April 2012 Director of HR / Secretary to Council

Risk 4: Loss of physical despatched to and held by third party for the delivery of their services (Data Security – Risk No 17.5)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
8	*Observation:* Applications are entered on to the NetRegulate system on arrival. Once entered the hard copy applications are picked up by Service Point who will scan and copy the documents with one	As planned, HPC should consider the introduction of online applications.	Housekeeping	Online applications are already on a project list, and will be prioritised when a suitable window in the	Ongoing Director of Operations/EMT

	copy being sent back to HPC and an electronic copy being sent on disk. A copy of the paperwork will be sent on to assessors for evaluation. Through discussion with the Head of Registration he confirmed that the current process is not ideal and informed us that HPC are currently looking at a project to consider introducing online applications. Whilst there would still be a requirement for certain proof of identity documents to be sent through the post, this would significantly reduce the current process which in turn would reduce the risk to potential information security breach. *Risk:* Ineffective processes resulting in an increased risk of information security breach.			projects schedule allows. However, we are legally required to provide a paper application above.	

Follow up of previous recommendations (report dated September 2011 – considered at Audit Committee 29 September 2011)

	Observation/ Risk	**Original category**	**Original management response and update response as of September 2011**	**Implementation date and manager responsible**	**Status**	**Comments/ implication**	**New recommendation**
1	Management should complete	Medium	Agreed. The system changes are	Sept 11	The agreed	The implementation date for this	Management should complete the steps

	the steps necessary by September 2011 towards removing the option for individuals to follow manual procedures when raising supplier purchase orders.		required for both PRS and Sage to ensure that the full benefits are realised and to ensure cross product compatibility. This should be implemented in the FY 2011/12, subject to budget approval.	Director of Finance	date for implementation of the recommendation has not yet been reached	recommendation had not yet been reached at the time of carrying out this audit. However, the upgrades required have been delayed until next year. HPC are currently undergoing several projects involving systems upgrades including major projects relating to Case Management and Fitness to Practice in anticipation of taking over responsibilities relating to GSCC and these have been prioritised.	necessary towards removing the option for individuals to follow manual procedures when raising supplier purchase orders. (Significant) **Updated management comment:** It is proposed to introduce the required changes as part of a major project in 2012/13 Financial Year but will need to be after the Social Work on-boarding major project.
2	Council should be provided with details of the number and type of health & safety incidents that have arisen at the HPC at least once annually.	Low	Agreed. August 2011 - Recommendation has not yet been implemented.	May 2011. Facilities Manager.	The recommendation has not yet been implemented.	Currently, this recommendation has not been implemented. We were advised HPC's agenda has been busy with a major focus being	The Council should be provided with a Health & Safety Report at least annually. This should detail: - health and safety activities over the previous year; and

						preparation for the transfer of regulatory functions from the GSCC to the HPC, currently anticipated to take place on 1st April 2012. However it is accepted that an annual Health & Safety Report is good practice and it is planned that one will be presented to the Council at the next opportunity.	- provide details of the number and type of health and safety incidents and near-misses and resulting lessons learned and action plans. (Housekeeping) **Updated management comment:** Noted. It is proposed to present a paper at December 2011 Council meeting. **Update:** The paper was presented to the December 2011 Council meeting.
3	The HPC's Human Resources (HR) Strategy should be updated to reflect the organisation's current thinking on its human resources	Medium	Director of Human Resources to update the HR strategy by April / May 2011.	May 2011 Director of Human Resources	Progress has been made on implementation of the recommendation	The Human Resources Strategy has been updated to reflect HPC's requirements including skills and training needs. We were informed the Strategy will be presented to the	As planned, the updated Human Resources Strategy should be reviewed and approved by the Finance & Resources Committee. (Housekeeping) The updated Human Resources Strategy was

	requirements, including skills and training needs.					Finance & Resources Committee meeting in September 2011 for approval.	approved by the Finance and Resources Committee on 7 September 2011 and is on the agenda for the Council meeting on 22 September. **Update:** The strategy was approved by the Council on 22 September 2011.

Partners (report dated September 2011 – considered at Audit Committee 29 September 2011)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	**Number of recommendations**
Fundamental	None
Significant	None
Housekeeping	1

Risk 3: Health & Safety of Partners (Risk No 6.3)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/responsibility**
1	*Observation:* An health and safety update is verbally delivered by a member of staff delivering the	HPC should review its risk mitigation controls	Housekeeping	Health and Safety information provided to partners is under	Nov 2011 Partner Manager/

	introduction of a course or hearing. There are no records as to who receives the update/briefing or a structured format of the content being delivered. Consequently there is no formal record maintained in support of this as a mitigating control on the HPC Risk Register. Another mitigating control in the Risk Register is 'Efficient and effective support and communication from the Partner team'. However there is no framework as to what mechanisms this control entails. *Risk:* Unclear and\or unambiguous controls within the Risk Register.	in relation to Partners to ensure these are clear and can be evidenced in practice.		review and guidance will be produced and incorporated into partner induction packs and/or the partner handbook. This mitigating control in the risk register will be deleted and replaced with 'Effective appraisal and monitoring of reappointment processes'	Building Manager/ HR Director **Update**: A health and safety briefing sheet is now provided to partners at all hearings and training events that they attend Oct 2011 Partner Manager/ HR Director **Update:** The risk register has been updated

Core Financial Systems – Payroll (report dated September 2011 – considered at Audit Committee 29 September 2011)

Assurance on effectiveness of internal controls: Substantial Assurance

Recommendations summary

Priority	**Number of recommendations**
Fundamental	None
Significant	None
Housekeeping	3

Risk 3: Financial losses arising from fraud or error, inefficient processing or inappropriate activity (such as ghost employees, payment of staff who no longer work at the Council, authorised payments, etc)

	Observation/Risk	**Recommendation**	**Priority**	**Management response**	**Timescale/ responsibility**
1	*Observation:* In review of a sample of 20 'acting-up payments' made in the current financial year it was noted: - In one case (employee reference 313) an allowance had been correctly calculated and pro-rated for the part of May 2011, however, in June 2011 the pro-rated amount was paid again rather than a full month resulting in an underpayment of £57.68; - of the nine members of staff for which the payments related to, six received	The underpayment of £57.68 should be corrected in the next payroll run. Care should be taken to ensure that the correct acting-up allowance is paid. The Employee Handbook should	Housekeeping Housekeeping	Item noted. Correction was made in following month. Noted. Policies have been reviewed and employee	N/a N/a.

	15% of their employee's salary in their substantive position as stated in the Employee Handbook. In the remaining three cases one member of staff received 20% and two received 5%. During the audit we were informed that the Acting-Up Allowance policy is currently being reviewed and updated. *Risk:* Acting-Up Allowances are not correctly calculated or paid potentially resulting in financial loss and / or reputational damage.	be updated to reflect the practice of acting-up allowances not always being paid at 15% of the salary of the employee's substantive position. In addition, the sections relating to Overtime /TOIL and Redundancy should be updated when these policies are reviewed.		handbook was updated in August 2011.	
2	*Observation:* Finance receive an HR Pack on a monthly basis which includes the HR Summary spreadsheet and relevant supporting documentation detailing starters; leavers; contractual variations; acting-up allowances; changes to address etc. Whilst our review confirmed that this information was received by Finance, in a timely manner and before the deadline of the 15th of the month, as there is currently no direct interface	As part of the planned review of the HR system, consideration should be given to a more effective interface between the HR and Payroll systems to avoid duplication in entry of data.	Housekeeping	Project proposal to review HR & partners information systems, including link to payroll to be submitted to Executive team in November 2011. If agreed will form part of 2012/13 project plan.	Director of Finance/ HR Director. Timescales pending outcome of Executive Team meeting November 2011 **Update**: The project proposal for review of HR and Partners information systems has been approved

	between the HR Systems and Sage, the information has to be entered again on to Sage. It is noted that a review of the HR system is planned to be undertaken. *Risk:* Holding two databases with staff details and duplication of data entry are unlikely to be an efficient use of resources. Errors are more likely to arise where data is re-keyed.				and includes a link to payroll. The project is currently scheduled to commence in the latter part of 2012/13.