BRITISH TRANSPORT POLICE

Agenda Item 5

REPORT TO:	**Audit & Corporate Governance Committee**
DATE:	**30 June 2009**
SUBJECT:	**Follow up to Previous Audit Reports**
AUTHOR:	**Principal Accountant**
SPONSOR:	**Director of Finance & Corporate Services**

1. PURPOSE OF PAPER

1.1 To update the Audit & Corporate Governance (A&CG) Committee on further work carried out to follow up implementation of recommendations arising from Audit Reports issued in previous years.

2. BACKGROUND

2.1 A report is brought to each meeting of the A&CG Committee outlining progress against findings in previous audit reports. All audit recommendations are given a risk factor of high, medium or low - this update covers all findings except those categorised as low risk.

2.2 This report gives members an update on the outstanding action points from the 2007-08 and 2008-09 Audit Plans It gives details on the status of the recommendation, the deadline for completion and the ongoing work to ensure that the recommendation is implemented by the stated deadline.

3. UPDATE ON IMPLEMENTATION OF AUDIT RECOMMENDATIONS

3.1 Monitoring of 2007-08 Audit Recommendations

All audit reports relating to 2007-08 have been presented to this Committee and, at the date of last report, there were two outstanding high and medium risk recommendations as detailed in Appendix A. Both of these matters have now been completed.

3.2 Monitoring of 2008-09 Audit Recommendations

All audit reports for the 2008-09 accounting year have been presented to this Committee and, at the date of the last report, there were seven outstanding high and medium recommendations as detailed in Appendix B. Two of these have been completed and five remain outstanding.

4. FINANCIAL IMPLICATIONS

4.1 There are no additional financial implications arising from this report.

5. DIVERSITY ISSUES

5.1 There are no diversity issues associated with this report.

6. RECOMMENDATIONS

6.1 It is recommended that the progress on the outstanding internal audit recommendations in this report is noted.

APPENDIX A

Follow up to 2007-08 Audit Recommendations

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
07-08-11 **Business Continuity Review**	The business impact analysis (BIA) should be revisited and drawn up to record appropriate information to drive an informed response to a disaster scenario. The BIA should contain a detailed analysis of critical services. The objective will be to identify the most critical services that the Force should restore in a disaster scenario, the order in which they should be restored, and the underlying resources required. The BIA should be drawn up in conjunction with key stakeholders, potentially through a facilitated workshop, so that critical services, resources and responses can be agreed and verified. ICT should be contacted in order to understand whether they are able to restore required technologies within the required time. Business continuity plans should be aligned to the BIA so that resources are directed appropriately to restoring key services in a timely manner.	The Business Continuity Institute to be contacted to determine “good practice” in the field of Business Impact Analysis documentation. A revised Business Impact Analysis document to be drafted and reviewed by an appropriately qualified MBCI, in accordance with BS 25999. Responsibility for action: Force Civil Contingencies and Business Continuity Manager on appointment. (Interim responsibility with the Chief Inspector Civil Contingencies)	This item is subject to a separate report on the agenda.	**COMPLETED**	June 2009
07-08-11 **Risk Management Review**	The Force should ensure that all key partnerships have appropriate and effective risk management arrangements which are aligned with the Force’s approach to risk management. Risk management guidance should be updated to include guidance on the management of risk in partnership.	BTP had already identified this as an area for attention during 2008/09 as a recommendation from the Risk Management Health Check completed by the IIA on 8 February 2008. Work is planned to start once the permanent Risk Management Coordinator starts (16th June 2008) and will include consideration of development of a SOP for partnerships.	A guidance document on partnership risk issues is in place using the national guidance produced by the Police Sector Group of ALARM.	**COMPLETED**	June 2009

Follow up to 2008-09 Audits

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
08-09-10 **LU Area**	Design of Controls – Lack of up to date policies & Procedures All draft procedure notes should be reviewed to ensure that they provide sufficient details of the key controls and procedures including authorised signatories and responsibilities for finance officers in L area. Once approved, these should be made available via the shared drive/intranet to all relevant members of staff. New staff should be provided training in the processes they are responsible for undertaking, whilst staff currently in post should also be granted training to improve their competences and skills. Details should be provided by FHQ to L Area in relation to payments settled on their behalf. This will enable L Area to check that duplicate payments have not occurred.	All currently available draft policies and procedures to be revisited in line with accepted BTP and LUL policies and procedures to ensure they define the relevant processes in sufficient detail and be duly approved by the Head of Finance & Corporate Services (HOFCS). Also further procedures are to be drafted to include such items as Devolved Budgets and Authorised Signatories. Once approved by the HOFCS the procedures will be published as recommended. Whilst there has been a significant improvement in the interaction between FHQ and L Area Finance sections on the inter area cross charging Agency Account, both through more two side communication and period by period meetings with agreed and written up action points, there will be future work to better document and reconcile charges made, especially by FHQ. Additionally it is important that both area and FHQ adhere to the agreed Agency Account Policy & Procedures.	“L” Area operates within the financial systems of LUL and TfL. This provides a robust control environment. In addition, BTP FHQ provides additional reassurance. However, there is a steadily improving control environment within “L” Area. Draft procedures covering a range of topics are on the “L” Area website. Over time additional guidance will be made available and the website improved. Regular meetings take place regarding recharges from FHQ and the charges are subject to comprehensive reconciliations. In summary, strong controls exist and have been improved. Work continues to make them more efficient.	**COMPLETE**	March 09

Agenda Item 5

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
08-09-12 **Corporate Governance**	**Risk Management Strategy** The Authority should seek to align the its risk management approach with the Force's using the principles of the Force's standard operating procedures for risk management which have already been developed. This should be codified in a joint risk management strategy which sets out how the risk management process at the Force and the Authority is to function. The Force risk management Coordinator should meet regularly with the Authority Treasurer to review risks and management action which may impact the Authority and the Force. The Authority's strategic risks should be presented alongside the Force's strategic risk register at all Audit and Corporate Governance Committee meetings.	The secretariat receives the agenda and papers for CAG and attends the meetings. BTP had already identified this issue as an area of concern and attempts had been made to meet with the Authority prior to the audit. We will work to establish a common approach to risk management. The BTPA Treasurer is to meet with Kay Black to determine the strategy going forwards including necessary meetings. The Authority's risk register will be presented quarterly at the Audit and Corporate Governance meeting alongside the BTP Risk Register.	The structure was completed by April 2009 and the first Risk Committee will be held in July 09.	**COMPLETE**	April 2009
08-09-10/11 **Force Control Room, Birmingham and Call Handling System**	**Disaster Recovery Plan** Management should ensure that the updated disaster recovery plans are documented ahead of the project closure. The results of the tests should be documented and used to provide a check on the effectiveness of the plans and the results of testing prior to sign off. Responsibility for the	The disaster recovery functions have been tested and we are confident that other than some catastrophic failure of the telephony system outside of BTP's control i.e. within Global Crossings exchange there is no risk to BTP. Disaster recovery test results will be formally documented and assigned responsibility of the application	A disaster recovery plan has been implemented and is owned by each Control Room Manager.	**COMPLETE**	March 2009

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
	maintenance of the plans should be assigned to an appropriate individual.	owner. This issue is considered to be of low risk to the Force			
08-09-07 **Data Security**	**Control Design – Portable Storage Devices** Usage of portable devices should be restricted by ensuring: Only portable storage devices issued by the Force can be used on the Force's computer equipment. This can be achieved with the implementation of port lock down software. Other potential storage devices (for example, fire wire and infrared ports which can be found on most laptops and be used to transfer data) should also be considered. All USB memory sticks issued to employees have security features such as encryption enabled. CD writing capability is limited to those who have a business need to perform this activity.	Policy and procedures in place governing both usage and acceptable types of portable storage devices. New Software Hitachi Vigilance Pro to be implemented to govern port access.	This is one strand of the ongoing IMPACT Project. Currently the new software is on schedule to be implemented in the majority of docking ports by August 2009.	Ongoing	**Deadline for action**: Implementing Hitachi Vigilance Pro will provide the facility to monitor and audit the moving of data from Force system to portable storage devices (memory sticks, CDs, portable hard drives etc). It will also provide the facility to control, including prevent, users being able to access any portable storage device from Force systems. The general setting will be to prevent access to most devices. In order to prevent these enhanced controls having an adverse impact on day to day operations, the implementation project will include surveying users to find out who has a legitimate requirement to export data on portable devices. A communication strategy will also be developed to ensure all staff are aware of the new control mechanisms and the process to request access. The existing policy and SOP should cover the use of Hitachi Vigilance Pro, but these will also be reviewed. Fundamentally there will be very limited access to portable storage capability and where it is legitimately

Agenda Item 5

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
					required, it will be closely monitored and controlled. September 2009

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
08-09-07 **Data Security**	**Control Design – Regulatory Compliance Monitoring** The Force should proactively monitor adherence to regulatory requirements such as the Data Protection Act. We recognise that the Force is currently undertaking the implementation of the mandatory measures recommended by the Management of Police Information (MOPI) guidance.	The force should be complying with ACPO Data Protection Manual of Guidance Part 1 and 2 which includes monitoring and audit.	This is also part of the IMPACT Project. Work is underway to ensure that BTP complies with MOPI, including briefing staff on the implications, before monitoring commences.	Ongoing	September 2009.
08-09-07 **Data Security**	**Operating Effectiveness – Electronic Data Transmission** The Technology department has recently acquired a module which can monitor data being transmitted based on definitions by the organisation. This module should be implemented with the assistance of the Information Security and Data Protection Officers to ensure that restricted and confidential data is being transmitted via the appropriate channels. Furthermore, the Force should consider implementing measures, such as data masking, to control the copying and sharing of restricted and confidential data. This will reduce the risk of	Policy and procedures exist which strictly forbid the emailing of protectively marked information to non BTP or Police email addresses.	The policy and procedures are written, the actual audit forms part of the IMPACT programme.	Ongoing	**Deadline for action**: Dip sampling will be conducted by Technology on a fortnightly basis to identify attachments going out to non PNN addresses and to examine these attachments to ensure that they do not breach Force Policy and Procedures. September 2009

	inadvertent disclosure or loss brought about by multiple copies of the same data.				

Reference	Recommendation	Initial Response	Updated Response	Current Status	Deadline for Completion
08-09-04 **Payroll Review**	Control Design – Updated Policies & Procedures The payroll procedures should be reviewed and updated to reflect the changes following the implementation of Trent. All staff involved in the payroll process should be briefed on these changes and the procedures made available on the shared drive.	Payroll procedures exist as far as operating the TRENT payroll system is concerned and individual guidance notes are available for various aspects of the administrative arrangements, document flow etc that surround payroll operations. It is accepted that a comprehensive review of these processes should be undertaken so that they are brought together in one document. This is being undertaken as part of an overall review of Finance Department Procedures.	While drafts of a number of these procedures are now in place, the formal versions are yet to be finalised.	Deadline for completion moved from June to September 2009.	September 2009