

Board Meeting Paper	
May 14 BM 11.0	
Purpose of report	<input type="checkbox"/> Decision ¹ <input type="checkbox"/> Discussion / debate <input checked="" type="checkbox"/> Information only ²
Sensitive Information?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
If sensitive, protective marking³	
Date of Meeting	15 May 2014
Agenda Item	11
Report Title	Half yearly risk report
Sponsor	Marian Lauder
Author(s)	Jon Carter



1. Summary
<p>This half yearly report to Board covers those aspects of risk management within the Audit Committee's oversight. It is a requirement of its terms of reference that the Committee reports to the Board twice a year.</p>
2. Recommendations for action
<p>This report is for noting only</p>
3. Serious risk management issues this half year
<p>None identified</p>

4. Risk issues reviewed			
The Committee has reviewed the following aspects of the risk management system this half year:			
Element	Owner	Date last reviewed	Comments
Corporate risk register	Jon Carter on behalf of management team	16/01/14 & 10/04/14	The assessment of risk against the top 7 objectives continued to be useful in achieving a common understanding amongst management team members of the main programme risks and associated mitigating actions. The top corporate/strategic risks are still rightly focused on ability to influence and risk to reputation. Succession planning remains a separate risk and the development of a succession plan should commence in Q1, and will be the subject of an internal audit in 2014-15.

¹ If a decision is required, or you are asking for the paper to be formally noted, please set this out in section 2

² If for information only, please make clear in section 1 **why** this information is being provided

³ ie **OFFICIAL/SENSITIVE**: plus COMMERCIAL / POLICY / MANAGEMENT-STAFF / PERSONAL PROTECT

Team risks: Resources Team	Nigel Holden	16/01/14	NH described the measures he was taking to mitigate against the risks he had identified for the resources team which the committee noted. NH undertook to consider how equalities training could be provided for board members.
Team risks: Research Team	Ian Wright	16/01/14	IW introduced the key risks facing the research team. Good controls were in place in respect of the integrity of research, which was important now that third party funding was growing so rapidly. On resourcing, one member of staff was due to leave shortly and he was considering an interim appointment in the short term whilst he reviewed the overall structure of the team in light of emerging demands placed on it.
Team risks: Passenger Issues Team	Mike Hewitson	10/04/14	MH discussed the PIT risks with the committee. Among these (PIT09) was that of resourcing the work on franchise replacement – many rounds of discussions with bidders and stakeholders as well as reviewing aspects of bids – for which funding had not yet been agreed.

Team risks for the remaining teams were reviewed in Q3 and will next be reviewed in Q3 2014-15.

Mid year management assurance return to DfT	Jon Carter	16/01/14	The committee noted the update from DfT explaining the delay in this process to the end of Q3.DS reported that the commissioning note had in fact arrived the previous day with a deadline return date of 7 February, which was achieved.
Triennial review	David Sidebottom	16/01/14 & 10/04/14	In January, ML/DS reported on the progress of the TR working group which had met the previous day. The board had been informally briefed that morning. The group had been very impressed with the review of achievements over the previous three years, compiled by Jon Clay, and had commissioned a review of the consideration given to alternative delivery models from Jon Carter. In April, following a written ministerial statement about which Passenger Focus was not forewarned, the committee learned that the review would be largely governance focussed and take place later in the year.

5. Information Risk

The Committee also keeps a watching brief on information risk issues as it is required to do by IA Standard No 6 (protecting personal data and managing information risk) of HMG Security Policy Framework and compliance with the Freedom of Information Act 2000 and the Data Protection Act 1998. The Senior Information Risk Owner (SIRO) (Jon) provides the Committee with a quarterly report.

Q	Date considered	Issues Comments
4	10/04/14	<p>The committee recalled it had been informed on 10 February (following the Connect announcement attached at annex A) regarding a data incident involving January payslips for the London office. These were, as usual, mailed from Manchester to London but were, unusually, interfered with en route. We became aware of the issue on Monday 3 February after some staff reported that their slips had arrived at home bearing an unenforced excess postage stamp, and others reported an excess postage demand card with the payslip being retained at the local delivery office.</p> <p>Consultations with Messrs Royal Mail proved nothing: the envelope had presumably been damaged and the contents delivered into a postbox.</p> <p>These payslip documents attract our protective marking RESTRICTED: PERSONAL PROTECT. This is because they contain information which links one or more identifiable living person with information about them whose release would put them at significant risk of harm or distress. I've underlined the relevant data.</p> <p>In other words,</p> <p><u>Name</u> / <u>addresses</u> (home or business or both) / <u>postcode</u> / email / telephone numbers / driving licence number / date of birth [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]</p> <p>Combined with:</p> <p>Sensitive personal data as defined by S2 of the Data protection Act, including records relating to the criminal justice system, and group membership, DNA or finger prints / <u>bank, financial or credit card details</u> / mother's maiden name / <u>National Insurance number</u> / Tax, benefit or pension records / health records / employment record / school attendance or records / material relating to social services including child protection and housing</p> <p>We are not aware of any harm or distress (beyond annoyance / frustration) and of course anyone who gets a bank statement by post is in the same position. However, as the conveyors of the data we have a duty of care and OUR envelope was interfered with. We have taken a number of steps:</p>

		<p>1. Shahid immediately posted a message on Connect</p> <p>2. Future payslip mailings will be protectively marked and delivered under signed-for-on-delivery conditions</p> <p>3. Options suggested by CGI (our payroll provider) and discussed at Staff Forum included:-</p> <ul style="list-style-type: none"> • Sending by post in the same way (ie they are all delivered to her and then posted to London staff) but the payroll agency can remove bank details and NI number. However, if someone changed their bank details, they would still appear on the first payslip after the details were changed. • An on-line system • Sending all payslips by post from CGI in individual envelopes direct to employee's home addresses. • Having one package sent to London and one to Manchester direct from the payroll agency. <p>(LGC undertook to check costs of each and report back)</p>
--	--	--

5. New developments / other issues
None

6. Overall opinion
The Committee's overall opinion on the management of risk is set out below.

Rating	✓	Audit Definition
Full		Systems of corporate governance, risk management and internal control are fully established, documented and working effectively.
Substantial	✓	Systems of corporate governance, risk management and internal control arrangements are well established and working effectively. Very minor control weaknesses have been identified in a maximum of one or two discrete areas.
Reasonable		Systems of corporate governance, risk management and internal control arrangements are generally established and effective, with some minor weaknesses or gaps identified.
Partial		Systems of corporate governance, risk management and internal control are present and operating effectively except for some areas where material weaknesses or significant deficiencies have been identified, aspects of the control arrangements need documenting, or evidence does not exist to demonstrate effective operation.
None		Systems of corporate governance, risk management and internal control are poorly developed or non-existent or major levels of non-compliance or non-conformance have been identified. Control arrangements are not adequately documented, or evidence does not exist to demonstrate effective operation.