

	PAPER NO: AC.23(12)	
Board/Committee:	Audit Committee	
Date:	20 June 2012	
Paper title:	Internal Audit – Risk Management	
Author:	PricewaterhouseCoopers	
Executive sponsor:	Richard Flatman, Executive Director of Finance	
<b>Recommendation by the Executive:</b>	The Executive recommends that the Audit Committee note the attached report.	
Aspect of the Corporate Plan to which this will help deliver?		
Matter previously considered by:	N/A	On:
Further approval required?	N/A	On:
Communications – who should be made aware of the decision?	N/A	

**Executive summary**

The internal audit report on Risk Management is attached. The overall report was given a 'Medium Risk' rating.

The committee is requested to note this report.

**Attachment:**

- Risk Management report

## 1. Executive Summary

<p><b>Department:</b> Executive  <b>Audit Sponsor:</b> Richard Flatman  <b>Distribution List:</b> Martin Earwicker, Richard Flatman, Darrell Pariag and Ravi Mistry.  <b>Date of last review:</b> March 2010</p>	<p><b>Overall report classification</b></p> <p><b>Medium Risk</b> </p> <p>See section 3B for overall report classification criteria</p>	<p><b>Direction of Travel</b></p> <p>The previous internal auditors reviewed risk management in 2010 and concluded with Substantial assurance. The categories of conclusion are not directly correlated and thus a direction of travel can not be confirmed.</p>	<p><b>Control Design findings identified</b></p> <p><b>0</b> Critical risk  <b>0</b> High risk  <b>2</b> Medium risk  <b>0</b> Low risk  <b>0</b> Advisory</p>	<p><b>Controls Operating in Practice findings identified</b></p> <p><b>0</b> Critical risk  <b>0</b> High risk  <b>2</b> Medium risk  <b>0</b> Low risk  <b>0</b> Advisory</p>
--	---	--	--	--

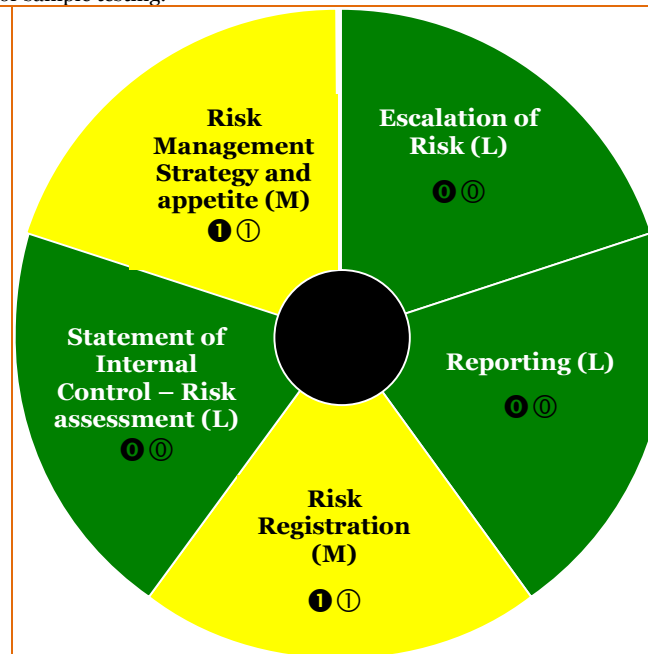
**Scope of the Review:** We have reviewed the design and operating effectiveness of key monitoring controls in place relating to risk management during the period 2011/12.  
**Limitation of scope:** Our work has been limited to that outlined within the terms of reference (attached), and all other areas have been excluded from our scope. This review did not look at the detailed operations of risk management within departments, other than those selected for sample testing.

**Summary of findings (See section 3A for individual finding ratings criteria):**

There are four medium risk findings:

- The nature of risks included on the corporate risk register were reviewed and it was noted that some of the risks as described in the corporate register are not directly controllable by the University. Management should focus on the risks that are within their control where they can take action to mitigate those risks occurring.
- There is no definition of risk appetite to help determine the level of risk the University is prepared to accept and therefore the extent of mitigating controls needed to address risks identified. **Appendix 5** outlines an example of risk reporting formats advised by Her Majesty's Treasury (HMT) for management information.
- The risk strategy document is the only place to communicate messages related to risk. This document could include reference to roles and responsibilities in more detail, as per HEFCE guidance.
- From a sample of five departmental risk registers, all had incomplete fields and some had information missing from entire columns, such as the "Cause and Effect". "Existing Controls" and "Action Required" columns. In addition, registers had not been updated on a timely basis, e.g. one register had not been updated since April 2010.


Value for money should be considered as part of the risk management process and mitigating controls put in place to the extent it is cost effective to minimise risk. At present there is room to improve LSBU's performance in this area.






Each of the sub processes for this review is shown as a segment of the wheel. The key to the colours on the wheel is:

- No/Advisory/Low risk Design of Controls or Controls Operating in Practice Issues identified (L)
- Medium risk Design of Controls or Operating in Practice issues identified (M)
- High risk Controls Design or Controls Operating in Practice issues identified (H)
- Critical risk Controls Design or Controls Operating in Practice issues identified (C)

## 2. Detailed Findings Recommendations and Action Plan

Finding	Potential Risk Implications	Recommendations	Finding rating	Management Response and agreed actions
<b>Inclusion of appropriate risks –Control design issue – Risk registration</b>				
<p>1 We noted from a review of the corporate risk register that it included risks which were not owned directly, and could not be actively managed by the relevant Faculty or Department.</p> <p>For example, the corporate risk register includes a risk that there may be a;</p> <p><i>‘Failure to position the University to effectively respond to changes in government policy and the competitive landscape’.</i></p> <p>The risk is included at an inherent risk rating of 4 (4 being the highest risk).</p> <p>The Universities commitments are laid out in the LSBU - 2011-14 - Corporate Plan. These commitments focus on growth, local accessibility to education, enterprise led research and VFM. The strategic risks threatening achieving these objectives are likely to relate to failure to adequately forecast income and balance expenditure so as to ensure the financial viability needed to service the Corporate Plans objectives. Furthermore, to be meaningful the risks need to be controllable by mitigating action.</p> <p>A general risk around failure to position the University to something as broad as government policy is meaningless since it cannot be aligned with mitigating action.</p> <p>A more appropriate interpretation of risk would be for the University to consider the consequence of “failing to develop a complete and accurate budget forecast within the context of likely government caps on fees and the impact on the Universities financial performance”.</p> <p>Control of this risk can be achieved since management can conduct sensitivity analysis around student income levels up to the maximum anticipated fee and corresponding likely student numbers at that fee level. Further control can then be added by management conducting a market comparison to determine the scope for the University to attract students in preference to other institutions at each fee level to inform a charging structure to help mitigate the risk that income does not meet budget.</p> <p>Even more control can be added by bottoming out the full budget position by detailed expenditure review. Risks around budget forecast inaccuracy are minimised where costs are completely understood and matched correctly to revenue streams so that profit, loss and breakeven positions are understood on a course by course level to help inform tactical and strategic decisions on course number and contribution. This analysis in turn helps inform strategy where the University has to condense courses around a market position and competitive identity e.g. cost leadership vocational courses or differentiated academic studies.</p> <p>By interpreting and linking risk in a very direct sense to objectives it is possible to determine mitigation and then scope to control the risk and Management and the Audit Committee are in a better position to assure the management action and accept or reject the risk.</p>	<p>Management may not be focused on addressing the risks that they can control.</p>	<p>Management should review their existing risks and look to focus on addressing the risks that are within their control.</p> <p>To assist with this and to ensure consistency of the risk registers, the quarterly meetings should continue to include review of a sample of Faculty/Department risk registers and consider whether they include risks which mitigate against achieving the Corporate Objectives of the University.</p>	<p> Medium risk</p>	<p><b>Agreed:</b> No – to be discussed further at Audit Committee.</p> <p>All risks on the corporate risk register are owned by a named member of the Executive team.</p> <p>We acknowledge that at corporate level some of these risks are quite broad. This reflects the fact that considerable recent effort has been made to make the process more manageable. Many of the more detailed risks were consolidated following the most recent internal audit report in risk in Spring 2010 which suggested that there were too many risks.</p> <p>Whilst the risk definition may be broad, the links to the corporate plan have been considered in detail and these are clearly identified such that each risk relates to specific objectives in the plan.</p> <p>Furthermore, the controls and action relate to specific issues which can be and are monitored very closely.</p> <p><b>Action to be taken:</b></p> <p>To be discussed further at Audit Committee. We will welcome further dialogue with the Internal Auditors to make improvements wherever possible.</p> <p><b>Responsibility for action:</b></p> <p>Corporate and Business Planning Manager</p> <p><b>Target Date:</b></p> <p>30 September 2012</p>

Finding	Potential Risk Implications	Recommendations	Finding rating	Management Response and agreed actions
<b>Lack of definition of risk appetite – Control design – Risk management strategy and appetite</b>				
<p>2</p> <p>Within the LSBU risk strategy document, it states that the Board of Governors role is with regard to setting risk appetite: ‘The Board of Governors has a fundamental role to play in setting the risk appetite of the University and in the management of risk’.</p> <p>At the time of the audit no risk appetite had been defined. It is acknowledged that risks are rated using a Red, Amber, Green (RAG) rating system, however this does not constitute a risk appetite.</p> <p>Without a clear articulation of risk appetite inconsistency in departmental risk interpretation cannot be managed.</p>	<p>There may be no guidance on which risks should be accepted, transferred, avoided and retained and so management may expend effort mitigating risks that are within the organisation’s risk appetite.</p>	<p>Management should define the University's risk appetite within the Risk Strategy.</p> <p>In addition, it is suggested that by defining a risk appetite there may be opportunity in the risk register to determine whether risk can be tolerated by the University.</p> <p>The TARA model - explained below - may be adopted to outline whether risks should be Transferred, Accepted, Retained or Avoided. This will clarify whether risks need to be mitigated and are controllable.</p>	<p> Medium risk</p>	<p><b>Agreed:</b> Yes</p> <p><b>Action to be taken:</b> A model will be developed as in the example provided for consideration by Committee and approval by the Board</p> <p><b>Responsibility for action:</b> Corporate and Business Planning Manager</p> <p><b>Target Date:</b> 30 September 2012</p>
<b>Deficiencies of the risk strategy – Control operating in practice - Risk management strategy and appetite</b>				
<p>3</p> <p><b>Roles and Responsibilities</b></p> <p>The risk strategy does not clearly set out roles and responsibilities and does not clearly set out governance arrangements (one paragraph exists on the role of the executive, one on risk champions and one for risk owners) in place with regard to Risk Management, despite both being key requirements of the HEFCE Risk Management guidance. Although roles and responsibilities are set out at a high level, there is no specific mention of responsible staff members and there is a lack of detail on structures in place below the executive level to manage risk within the University.</p> <p>Finally, there were no guidelines for reporting to external stakeholders included in the Strategy as recommended by the HEFCE guidance.</p> <p><b>Communication</b></p> <p>From both interviews conducted with departmental risk owners, there had been no training delivered to anyone who owns a risk and has access to 4risk (the University’s risk management system).</p> <p>In addition both heads of departments interviewed had not attended risk workshops to generate ideas for risk registers, as described as a key control by corporate risk management.</p> <p>It was noted from one of the two interviews with directors, that they were not aware of</p>	<p>There may be inadequate policies and procedure in place which undermine governance.</p> <p>LSBU may not comply fully with HEFCE Risk Management guidance. The risk control environment may not be strong and staff may not be aware of the policy in place.</p> <p>Risk owners may not be trained how to use 4risk and are not aware of the risk strategy.</p>	<p>Management should include greater detail of procedures and roles and responsibilities in the Risk Management Strategy document, or a separate document to ensure that HEFCE guidelines are met.</p> <p>The strategy should be communicated effectively by ensuring that training created by finance is delivered to all new risk owners and refreshed where changes to the strategy occur.</p>	<p> Medium risk</p>	<p><b>Agreed:</b> Partially – actions will be and are being continued to respond to this risk.</p> <p>The risk strategy has only recently been updated and we thought adequately documented the roles and responsibilities with regard to risk management processes.</p> <p>We have deliberately not been overly prescriptive in terms of process. However, we have provided the framework and tools to assist and training has been provided upon request. We have also been proactive in terms of offering training to users.</p> <p>There is no intention to hold central risk workshops to generate ideas for local risk registers. This is a responsibility of department heads themselves to ensure that their local registers are up to date.</p> <p>All staff should be aware of the risk strategy. It can be found on the Staff Gateway section of the university’s</p>

	Finding	Potential Risk Implications	Recommendations	Finding rating	Management Response and agreed actions
	the strategy document and did not know where to find this.				<p>website which is accessible by all staff.</p> <p><b>Action to be taken:</b></p> <p>We will review the HEFCE guidance and amend the strategy and/or produce a separate document as appropriate to ensure that the HEFCE guidance is met. A briefing note will be sent to all those responsible for risk management setting out their risk responsibilities.</p> <p><b>Responsibility for action:</b></p> <p>Corporate and Business Planning Manager</p> <p><b>Target Date:</b></p> <p>30 September 2012</p>
<b>Incomplete risk registers – Control operating in practice - Risk registration</b>					
4	<p><b>Incomplete fields in Risk registers</b></p> <p>It was noted that there was fields missing from all of the five departmental risk registers tested. For example, the National School of Bakery had empty fields for all of the risks within the ‘Cause and Effect’, ‘Existing Controls’ and ‘Action Required’ columns.</p> <p><b>Untimely updating of Risk Registers</b></p> <p>Three out of five departmental risk registers tested had not been updated on a timely basis. For example, the HR risk register had a risk which had not been updated since June 2011.</p> <p>There were examples acknowledged from interviews of risks on the risk register which were completed and risks closed, yet still included on the risk register. Thus reflecting that the registers were not up-to-date.</p>	<p>Risks may not be managed effectively and on a timely basis. Risk owners may not be aware of their responsibility as a risk owner.</p>	<p>Risk registers should be updated after every monthly meeting with Executive members to reflect changes and actions made.</p> <p>Monitoring of all risks at monthly meetings should be completed and updates added to the risk registers subsequently to reflect actions and changes of circumstance.</p> <p>Notes should be used on the 4risk system to indicate why changes have not been updated if applicable, or to show the closure of risk.</p>	<p> Medium risk</p>	<p><b>Agreed:</b> Yes</p> <p>The University risk processes already require departmental risk registers to be updated continually. This should not be an update after each Executive. It should be a continual process and should inform the updates to the Executive from each member of the Executive team. The letters of delegated authority make clear the responsibilities in this area. Whilst departmental risk registers are not reviewed in detail at the Executive, members of the Executive are required to raise key issues. The departmental registers are however reviewed at each of the quarterly review meetings.</p> <p><b>Action to be taken:</b></p> <p>The Executive team and all Heads of Department will be reminded of the importance of keeping registers up to date</p> <p><b>Responsibility for action:</b></p> <p>Corporate and Business planning Manager</p> <p><b>Target Date:</b></p> <p>30 April 2012</p>

# 3. Basis of our report classification and finding ratings





## A. Individual finding ratings

Finding rating	Points	Assessment rationale
<b>Critical</b>	40 points per finding	<p>A finding that could have a:</p> <ul style="list-style-type: none"> <li>• <b>Critical</b> impact on operational performance resulting in inability to continue core activities for more than two days; or</li> <li>• <b>Critical</b> monetary or financial statement impact of £5m; or</li> <li>• <b>Critical</b> breach in laws and regulations that could result in material fines or consequences over £500k; or</li> <li>• <b>Critical</b> impact on the reputation or brand of the organisation which could threaten its future viability, e.g. high-profile political and media scrutiny i.e. front-page headlines in national press.</li> </ul>
<b>High</b>	10 points per finding	<p>A finding that could have a:</p> <ul style="list-style-type: none"> <li>• <b>Significant</b> impact on operational performance resulting in significant disruption to core activities; or</li> <li>• <b>Significant</b> monetary or financial statement impact of £2m; or</li> <li>• <b>Significant</b> breach in laws and regulations resulting in significant fines and consequences over £250k; or</li> <li>• <b>Significant</b> impact on the reputation or brand of the organisation, resulting in unfavourable national media coverage.</li> </ul>
<b>Medium</b>	3 points per finding	<p>A finding that could have a:</p> <ul style="list-style-type: none"> <li>• <b>Moderate</b> impact on operational performance resulting in moderate disruption of core activities or significant disruption of discrete non-core activities; or</li> <li>• <b>Moderate</b> monetary or financial statement impact of £1m; or</li> <li>• <b>Moderate</b> breach in laws and regulations resulting in fines and consequences over £100k; or</li> <li>• <b>Moderate</b> impact on the reputation or brand of the organisation, resulting in limited unfavourable media coverage.</li> </ul>
<b>Low</b>	1 point per finding	<p>A finding that could have a:</p> <ul style="list-style-type: none"> <li>• <b>Minor</b> impact on the organisation's operational performance resulting in moderate disruption of discrete non-core activities; or</li> <li>• <b>Minor</b> monetary or financial statement impact £500k; or</li> <li>• <b>Minor</b> breach in laws and regulations with limited consequences over £50k; or</li> <li>• <b>Minor</b> impact on the reputation of the organisation, resulting in limited unfavourable media coverage restricted to the local press.</li> </ul>
<b>Advisory</b>	0 points per finding	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Each individual finding is given points, based on the rating of the finding (Critical, High, Medium, Low or Advisory). The points from each finding are added together to give the overall report classification of Critical risk, High risk, Medium risk or Low risk, as shown in the table on the next page.

## B. Overall report classification

The overall report classification is determined by allocating points to each of the findings included in the report

Report classification	Points
 <b>Low risk</b>	6 points or less
 <b>Medium risk</b>	7– 15 points
 <b>High risk</b>	16– 39 points
 <b>Critical risk</b>	40 points and over

**Responsibilities of management and internal auditors** It is management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems. We shall endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we shall carry out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected. Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations or other irregularities which may exist, unless we are requested to carry out a special investigation for such activities in a particular area. Our internal audit work has been performed in accordance with CIPFA's Audit Code of Practice. As a result, our work and deliverables are not designed or intended to comply with the International Auditing and Assurance Standards Board (IAASB), International Framework for Assurance Engagements (IFAE) and International Standard on Assurance Engagements (ISAE) 3000.

**Limitations inherent to the internal auditor's work** We have undertaken this review, subject to the limitations outlined below. Internal control, no matter how well designed and operated, can provide only reasonable and not absolute assurance regarding achievement of an organisation's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances. The assessment of controls relating to this review is for the period January to February 2012. Historic evaluation of effectiveness is not relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

**PricewaterhouseCoopers LLP Disclaimer** This document has been prepared for the intended recipients only. To the extent permitted by law, PricewaterhouseCoopers LLP does not accept or assume any liability, responsibility or duty of care for any use of or reliance on this document by anyone, other than (i) the intended recipient to the extent agreed in the relevant contract for the matter to which this document relates (if any), or (ii) as expressly agreed by PricewaterhouseCoopers LLP at its sole discretion in writing in advance.

In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000, it is required to disclose any information contained in this report, it will notify PwC promptly and consult with PwC prior to disclosing such report. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and London South Bank University shall apply any relevant exemptions which may exist under the Act to such report. If, following consultation with PwC London South Bank University discloses this report or any part thereof, it shall ensure that any disclaimer which PwC has included or may subsequently wish to include in the information is reproduced in full in any copies disclosed.

© 2012 PricewaterhouseCoopers LLP. All rights reserved. 'PricewaterhouseCoopers' refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) or, as the context requires, other member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.



## 4. Terms of reference

# *London South Bank University*

## *Terms of reference-Risk Management*

**To:** *Richard Flatman, Director of Finance*

**From:** *Justin Martin, Head of Internal Audit*

This review is being undertaken as part of the 2011/2012 internal audit plan approved by the Audit Committee.

---

### Background

Risk management can be defined as the culture, processes and structures that are directed towards the effective management of threats to the achievement of an organisation's objectives and/or barriers to an organisations exploitation of potential opportunities. Good risk management is a key element of good governance.

Risk management often has negative connotations, particularly the misconceived perception that it is a 'box-ticking' exercise, irrelevant to all but a few individuals in an organisation. This is incorrect and ignores the fact that risk exists at every level of an organisation, and as a consequence risk management is an ongoing responsibility for every member of an organisation.

Effective risk management has numerous benefits. These include:

- Reduced time spent 'fire fighting';
- Increased confidence moving into new areas, or undertaking new projects;
- Getting things right first time;
- Improved management information; and
- Protection of the organisation's reputation.

The ability of an organisation to successfully implement effective risk management arrangements in order to take advantage of these benefits is heavily dependent on staff and officers having an understanding of their responsibilities together with the principles and processes that underpin effective risk management. Only with this understanding will individuals buy-in to and engage with risk management, and help embed the arrangements into the culture of the organisation.

In the previous year, risk management was tested as part of other individual reviews. This year a more detailed review will of risk management will take place to ensure that LSBU is HEFCE compliant and managing risk effectively.



---

## Scope

We will review the design and operating effectiveness of key monitoring controls in place relating to Risk Management during the period 2011/12. The sub-processes and related control objectives included in this review are:

<i>Sub-process</i>	<i>Control objectives</i>
Risk Management Strategy and Appetite	Compliance with HEFCE risk management requirements Risk Strategy is reflective of the risk management operations and risk appetite of the University. The Corporate Risk Framework is comprehensive and up to date.
Statement of Internal Control – Risk Assessment	The Statement of Internal Control, risk assessment response is supported by robust and effective operations and controls.
Risk Registration	The Corporate Risk Register is a comprehensive record of risk facing the University. Where risks are not present on the Corporate Risk Register they are included in relevant departmental risk registers.
Escalation of risk	Risks are escalated from Departments to the risk corporate risk register on a timely basis. Risk registers are complete in departments and used as part of decision making (a sample of two departments will be assessed). Risks are reviewed regularly and removed where no longer relevant and the rationale for removing and / or downgrading risks is clear and documented.
Reporting	Risk reporting to the Audit Committee and the Board of Governors is timely and clear to ensure risk management can be owned by the non executive members of the University.

---

## Limitations of scope

Work will be limited to work outlined within these terms of reference, and all other areas will be excluded from scope. This review will not look at the detailed operations of risk management within departments, other than those selected for sample testing.

---

## Audit approach

Our audit approach is as follows:

- Obtain an understanding of the Risk Management process through discussions with key personnel, review of systems documentation and walkthrough tests;
- Identify the key risks through use of a Risk Rainbow tool to assess whether all risk categories have been considered by the University;
- Evaluate the design of the controls mitigating actions in place to promote risk management; and
- Test the operating effectiveness of the key controls mitigating actions around risk management.

---

## Internal Audit Team

---

<i>Name</i>	<i>Title</i>	<i>Role</i>	<i>Contact details</i>
Justin Martin	Engagement Partner	Partner	020 7212 4269
Debbie Tilson	Engagement Manager	LSBU Audit Manager	020 7804 0506
Clare White	Manager	Risk Management Specialist	07841569316
Louisa Metcalfe	Senior Associate	Risk Management Specialist	079151171590

---

## Key contacts – London South Bank University

---

<i>Name</i>	<i>Title</i>	<i>Role</i>	<i>Contact details</i>
Martin Earwicker	Vice Chancellor	Executive Board	martin.earwicker@lsbu.ac.uk
Chris Swinson	Chair of Audit Committee	Board of Governors	chris@swinson.co.uk
Richard Flatman	Executive Director of Finance	Executive Board/Finance	richard.flatman@lsbu.ac.uk
Darrell Pariag	Corporate and Business Planning Manager	Finance	pariagd2@lsbu.ac.uk
Ravi Mistry	Finance Systems Manager	Finance	mistryrm@lsbu.ac.uk

---

## Timetable

---

**Fieldwork start** 30/01/2012

---

**Fieldwork completed** 13/02/2012

---

**Draft report to client** 02/03/2012

---

**Response from client** 09/03/2012

---

**Final report to client** 16/03/2012

---

Agreed timescales are subject to the following assumptions:

- All relevant documentation, including source data, reports and procedures, will be made available to us promptly on request; and
  - Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.
-

# 5. Examples of risk reporting Formats

## Risk Dashboard

The risk dashboard included below provides an example of how risk appetite could be defined for each of the strategic risks faced by the University. Risks are represented pictorially, showing the appetite for each and their relationship to inherent (raw) and residual risk. It shows inherent and residual risk showing the impact of mitigating controls.

Source: 'Thinking about your risk – setting and communicating your risk appetite', HM Treasury © Crown copyright 2006.

