

Meeting of the Audit Committee

4.00 - 6.00 pm on Thursday, 22 September 2016
in 1B16 - Technopark, SE1 6LN

Agenda

<i>No.</i>	<i>Item</i>	<i>Pages</i>	<i>Presenter</i>
1.	Welcome and apologies		Chair
2.	Declarations of interest		Chair
3.	Minutes of the previous meeting (for publication)	3 - 10	Chair
4.	Matters arising		Chair
Internal audit			
5.	Internal audit progress report (to discuss)	11 - 28	PwC
6.	Internal audit report - data security (to discuss)	29 - 78	PwC
	• External infrastructure vulnerability assessment (to note)		
7.	Internal audit report - Prevent (to discuss)	79 - 100	PwC
8.	Internal audit report - risk management (to discuss)	101 - 124	PwC
9.	Continuous auditing, key financial systems (to discuss)	125 - 174	PwC
10.	Draft internal audit annual report (to discuss)	175 - 198	PwC
11.	Internal audit charter (to note)	199 - 206	PwC
External audit			
12.	Pensions assumptions (to approve)	207 - 216	CFO
13.	External audit sourcing strategy (to approve)	217 - 222	CFO
<i>In the absence of the external auditors</i>			
Risk and control			
14.	Corporate risk register (to discuss)	223 - 242	CFO
15.	Risk strategy (to recommend to the Board)	243 - 260	CFO
16.	Risk appetite (to recommend to the Board)	261 - 264	

<i>No.</i>	<i>Item</i>	<i>Pages</i>	<i>Presenter</i>
Other matters - items to approve			
17.	Annual review of effectiveness: statement of internal controls (to approve)	265 - 280	CFO
18.	Modern slavery Act statement (to approve)	281 - 288	Sec
19.	Corporate Governance Statement (to approve)	289 - 296	Sec
20.	Public Benefit Statement (to approve)	297 - 300	Sec
Other matters - items to note			
21.	Speak up report (to note)	301 - 302	Sec
22.	Anti-fraud, bribery and corruption report (to note)	303 - 304	CFO
23.	Audit Committee business plan (to note)	305 - 308	Sec
24.	Membership and Terms of Reference (to note)	309 - 314	Sec
25.	Matters to report to the Board following the meeting		Chair
26.	Any other business		
27.	Date of next meeting		

Date of next meeting - 4.00 pm on Thursday, 10 November 2016

Members: Steve Balmont (Chair), Shachi Blakemore, Mee Ling Ng and Roy Waight

Internal Auditors

External Auditors

In attendance

	CONFIDENTIAL
Paper title:	Minutes of the meeting of 9 June 2016
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Megan Evans, Governance Assistant
Board sponsor:	Steve Balmont, Chairman of the Audit Committee
Purpose:	To approve the minutes of the past meeting as a correct record and to approve for publication

Matter previously considered by:	N/A	N/A
Further approval required?	No	N/A

Executive Summary

The Committee is asked to approve the minutes of its meetings of 9 June 2016. There are no suggested redactions for publication on LSBU's website.

London South Bank University

Minutes of a Meeting of the Audit Committee
Held at 4pm on Thursday, 9 June 2016
In room V404, K2, Keyworth Street, London, SE1

Present

Steve Balmont	Chair
Shachi Blakemore	
Douglas Denham St Pinnock	
Mee Ling Ng	
Roy Waight	Independent co-opted member

External Auditors

Carol Rudge	Grant Thornton
-------------	----------------

Internal Auditors

Charlotte Bilsland	PricewaterhouseCoopers
Justin Martin	PricewaterhouseCoopers

In attendance

Prof David Phoenix	Vice Chancellor and Chief Executive
Richard Flatman	Chief Financial Officer
Craig Girvan	Head of ICT Security (<i>for minutes 1 – 9</i>)
Paul Ivey	Pro Vice Chancellor (Research and External Engagement) (<i>for minutes 1 – 9</i>)
Ian Mehrtens	Chief Operating Officer
James Stevenson	University Secretary and Clerk to the Board of Governors
Megan Evans	Governance Assistant
John Baker	Corporate and Business Planning Manager

Welcome and apologies

1. The Chair welcomed members to the meeting. The committee welcomed Roy Waight to his first meeting of the committee as an independent co-opted member.
2. Apologies had been received from Pat Bailey and Natalie Ferer. John Baker attended the meeting as an observer.

Declarations of Interest

3. No interests were declared on any item on the agenda.

Minutes of the last meeting

4. The minutes of the meeting held on 11 February 2016 and the redactions were approved (paper **AC.14(16)**). The minutes were approved for publication.

Matters arising

5. Minute 5 of 11 February 2016 – the committee noted that a formal journal review process was now in place.

Date Security closure report

6. The committee discussed the closure report and agreed to keep it as a live action as there are a number of ongoing actions. The committee will receive an update at the next meeting.

International Students audit report

7. The committee discussed the international students audit report from Penningtons Manches (paper **AC.16(16)**). It was reported that the audit shows sufficient preparedness for a UKVI audit.
8. The committee noted due to frequent rule changes from the Home Office changed frequently three additional staff members had been brought in to provide additional resource.
9. The committee noted the progress so far and discussed the cost of compliance.

Paul Ivey and Craig Girvan left the meeting

External audit plan 2015/6

10. The committee discussed the external audit plan (paper **AC.17(16)**), which was based on areas of risk. The committee noted that pensions liability was a significant risk; as well as the transition to FRS102 and new UK GAAP, which would pose a one-off significant risk. The committee requested an update on accounting policies.

Indicative pensions assumptions

11. The committee noted the indicative pensions assumptions (paper **(AC.18(16))**)
The committee noted that the LPFA assumptions would be brought back to the next meeting for approval.
12. Other matters discussed included the need to complete the technical review prior to the November meeting, the materiality level and measures against fraud.

Annual bad debt write-off (AC.19(16))

13. The committee approved the write-off of tuition fee debt of £625,000 (paper **AC.19(16))**).
14. The committee noted that the executive had agreed a change to the payment plan to commence from 2017/8 academic year, which would require students to pay their final instalment by 31 January each year, in line with sector practice.
15. The committee noted that LSBU makes effort to actively recover debt before referring the matter to collection agencies. The committee requested a review of how efficiently LSBU collects debt.

Progress report and reports from PwC

16. The committee noted the progress reports from PwC (paper **AC.20(16))**). The planned HR system pre-implementation review would now be carried out in the plan for 2016/17.

Financial data continuous auditing report, period 2

17. The committee noted the financial data continuous auditing report for period 2 (paper **AC.21(16))**). The amber rating for Payroll was due to a lack of documentation. The committee noted that action was being taken in this area.

Student data continuous auditing report

18. The committee discussed the student data continuous auditing report (paper **AC.22(16))**), which was rated as low risk.

Internal audit report: Management Information: Data Quality

19. The committee discussed “management information: data quality” (paper **AC.24(16)**), which was rated as medium risk. The committee noted that the new data management framework should address the issues in the report.

Internal audit plan, 2016/17

20. The committee discussed the draft internal audit plan (paper **AC.25(16)**). The plan was for 127 days over the year.
21. The plan included an audit of ICT and preparations for the HEFCE institutional visit in early 2017. The committee approved the Internal Audit plan for 2016/17.

Corporate Risk Register

22. The committee noted the corporate risk register (paper **AC.26(16)**)

Anti-Fraud policy review

23. The committee noted that the anti-fraud policy (paper **(AC.27(16))**) remained unchanged from last year. The committee approved the policy.

Anti-fraud, bribery and corruption report

24. The committee noted the report. (paper **AC.28(16)**)

Speak Up report

25. The committee noted the Speak Up report (paper **(AC.29(16))**). No new issues had been raised since the last meeting.

TRAC(T) return to HEFCE

26. The committee noted and ratified the TRAC(T) return to HEFCE. (Paper **(AC.30(16))**)

Audit Committee business plan (AC.31(16))

27. The committee noted its business plan. It was noted that the external audit contract was due for renewal, which would be added to the business plan for the next meeting.

Matters to report to the Board

28. The committee requested that the internal audit completion rates, external audit tender and the audit plan were reported to the Board. Additionally, the committee agreed to continue with the UKVI and data security audits and asked for these to be included in continuous audit reporting.

Any Other Business

29. The Chair reported that this was the last meeting for Douglas Denham St Pinnock, who would now chair Major Projects and Investment Committee. The committee thanked Mr Denham St Pinnock for his contribution to the committee.

Date of the next meeting

30. The committee that the next meeting would be held at 4pm on Thursday 22 September 2016.

The Chair closed the meeting.

Confirmed as a true record:

.....
Chair



Committee Action Points

15 September 2016

15:23:56

Committee	Date	Minute	Action	Person Res	Status	
Audit	09/06/16	10	Update on accounting policies	CFO		<input type="checkbox"/> Completed
Audit	09/06/16	11	Pensions assumptions to 22 Sept 2016 meeting for approval	CFO	On agenda.	<input checked="" type="checkbox"/> Completed
Audit	09/06/16	15	Review of effectiveness of collecting debt	CFO	On agenda for Nov 2016	<input checked="" type="checkbox"/> Completed
Audit	09/06/16	27	External audit tender plan	CFO	On agenda	<input checked="" type="checkbox"/> Completed

Page 9

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Internal Audit Progress Report: September 2016
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with an overview of the current progress against the Internal Audit Plans for both 15/16, and for 16/17.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	The internal audit plan relates to controls and processes that relate to the entire organisation, and provide assurance against all of the risk types within the Corporate Risk Appetite statement.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

100% of the agreed internal audit programme for 15/16 is now complete, with 15% of the programme for 16/17 already undertaken.

The progress overview accompanies four reports to committee, alongside the draft internal audit annual report, and the confirmed plan for 16/17 along with the internal audit charter.

15 agreed recommendations were followed up in this period, and 87% have now been implemented, with two still in progress. (*details in appendix 2*)

- The Committee is requested to note the report and the progress made.

London South Bank University

Internal Audit Progress Report 2016/17

September 2016

London South Bank
University

Table of Contents

<i>Overview</i>	4
<i>Reporting Activity and Progress</i>	5
<i>Appendix 1 – Plan Progress</i>	8
<i>Appendix 2 – Follow Up</i>	10
<i>Appendix 3 – Recent PwC Publications</i>	15

This report has been prepared by PwC in accordance with our contract dated 15/05/2015.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to the Higher Education Funding Council for England's (HEFCE) Memorandum of Assurance and Accountability (MAA). 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.

Overview

Progress Summary

We have completed 100% of our internal audit programme for 2015/16 and 15% of our internal audit programme for 2016/17, which is in line with the agreed profile for our work. An outturn statement detailing assignments undertaken and actual activity for 2015/16 is shown in Appendix 1.

For this Audit Committee, we present the following final reports:

- Prevent Duties;
- Risk Management;
- Information Security;
- Continuous Audit: Key Financial Systems Period One – 2016/17.

We also present:

- Our draft 2015/16 Internal Audit Annual Report;
- Our draft 2016/17 Internal Audit Charter.

Findings of our Follow Up Work

We have undertaken follow up work on actions with an implementation date of 31/08/2016 or sooner. We have discussed with management the progress made in implementing actions falling due in this period. Where the finding had a priority of low or advisory, we have accepted management's assurances of their implementation; otherwise, we have sought evidence to support their response.

A total of 15 agreed actions have been followed up this quarter. 13 of these have been implemented (87%) and two are currently in progress (13%). The outstanding findings relate to the 2014/15 Change Portfolio review. Progress details are summarised at Appendix 2.

Other Matters

In August we hosted six London South Bank University (LSBU) finance interns at our PwC Embankment Office where we introduced them to PwC, provided details on the PwC graduate scheme and invited three of our junior staff to share their first year of experience with a professional services firm.

As part of our regular reporting to you, we plan to keep you up to date with the emerging thought leadership we publish. Our Higher Education Centre of Excellence and the PwC's Public Sector Research Centre (PSRC) produce a range of research and are the leading centres for insights, opinion and research on good practice in the higher education sector. We have included a summary of key publications at Appendix 3. We are happy to provide electronic or hard copy versions of these documents at your request.

Recommendations

- That the Audit Committee **notes** the progress made against our 2015/16 and 2016/17 Internal Audit Programme.
- That the Audit Committee **comments** on our reports for Prevent Duties, Risk Management, Data Security and Continuous Audit: Key Financial Systems Period One – 2016/17.
- That the Audit Committee **comments** on our draft 2015/16 Internal Audit Opinion.
- That the Audit Committee **approves** the proposed 2016/17 Internal Audit Charter.

Reporting Activity and Progress

Final reports issued since the previous meeting

Prevent Duties – low risk

UK Higher Education Institutions (HEIs) have a statutory duty to uphold freedom of speech in their institutions as far as is practical within the law. This duty has come under pressure recently from the Government's Prevent Strategy and provisions in the Counter-Terrorism and Security Act 2015. LSBU created a Safeguarding Strategy which outlines their approach to wider student safeguarding and their Prevent responsibilities. The purpose of this audit was to review the strategy and validate the processes and controls in place. We identified two *medium risk* findings:

- HEFCE requires that HEIs outline their Prevent duties within their ICT policies. LSBU's ICT policy does not currently reference Prevent. We also noted that there are currently no filters on mobile devices - including phones, tablets and expert systems (media labs for example) - to block access to extremist materials or Prevent-specific filters within LSBU's network which could allow access to extremist websites. LSBU's Information Security team run a weekly report to identify the 25 "worst offenders" attempting to access blocked websites. This control could be strengthened by including Prevent-specific reporting.
- LSBU do not retain a centralised listing of external speakers and events affiliated with them. Lack of central oversight could lead to students being exposed to inappropriate speakers or events.

We also identified two *advisory* findings relating to plans for increasing student engagement and Prevent training for employees

Risk Management – low risk

Effective risk management is essential in helping any organisation to improve governance, focus decision making and achieve objectives. Risk management is ensured through maintenance of risk registers and an awareness of risk throughout within an organisation. HEFCE direction states that institutions are required to have effective risk management policies and processes that cover all significant risks, assess exposure and regularly monitor risk to ensure effective governance. The purpose of this audit was to review the controls in place at LSBU for risk management and mitigation.

We identified one *medium* finding:

- We tested a sample of five Professional Service Department (PSD) and School's operational risk registers to confirm that these were being fully completed and reviewed on a timely basis. We identified a number of instances where the risk registers did not appear to be complete, risks and actions weren't specific and required actions had not been implemented by the agreed completion date.

We identified two *advisory* findings where improvements could be made:

- We reviewed the Corporate Risk Register to confirm that it was complete, up-to-date and appropriately documented. We identified that mitigating controls were missing for two of the 14 risks.
- We reviewed the actions points from the annual business review meetings and business plans for a sample of five PSD's and School's. We found instances whereby the defined risks were vague and not 'true risks'. There were also a number of agreed actions without a person responsible assigned or a target completion date.

Data Security – high risk

IT controls are integral to protecting an organisation's information data and assets (physical and intellectual). The purpose of this review was to assess the design and operating effectiveness of controls over data security by reviewing progress made in high risk areas and to consider the controls in place over IP addresses.

LSBU's IT landscape has been undergoing a period of rapid change. While our risk rating is consistent with prior year, we recognise that a significant amount of work has been done to update and rationalise the logical and physical security controls in place. This includes linking the HR system with IT access so that leavers have their Active Directory accounts disabled automatically and the ongoing iTrent project which will allow an audit trail of all staff changes to staff access levels. Despite these improvements, a number of issues remain.

We identified two *high risk* findings during our testing of user administration and logical security. A number of these findings were also identified in the 2014/15 Data Security internal audit.

Logical Security

We tested to confirm that controls and processes have been established to ensure that logical security settings are appropriate and applied consistently across the LSBU IT environment. We found:

- Unencrypted USB's can be used to extract data from the LSBU's systems.
- Contrary to the Mobile Devices Policy, users are able to 'opt out' of encrypting devices.
- Desktops aren't encrypted unless this is specifically requested.
- We were unable to obtain a complete listing of laptops held by the LSBU as a central list is not maintained. The listing that we did obtain showed that 77 of the 398 laptops known to the LSBU (19%) were not encrypted.
- The password parameters applied to Active Directory (AD) accounts differs to the Account Management policy.
- Laptops communicate with the network in order to update the encryption on the laptop. We identified that 356 of the 398 laptops listed (89%) had not communicated with the network for over 100 days.

User Administration

We reviewed the processes in place around user administration to ensure that there are appropriate controls around set up, modification and removal of user accounts. We found:

- ICT are not notified when an individual has moved within LSBU and we were unable to obtain a listing of changes made to user access. We understand from management that it is likely that members of staff who've changed position retain access to data that they are no longer permitted to see.
- For our sample of 30 leavers tested, four leavers AD accounts were still active at the date of fieldwork.

We identified one *medium risk* finding:

Physical Security

- We reviewed the procedures and controls in place to ensure the physical security of LSBU's buildings and associated IT assets. We visited five ICT storage areas to confirm that these were only accessible to specific ICT staff and found two of the buildings had active ICT network equipment that was not appropriately restricted.
- We tested the controls in place for providing security passes to staff. Forms could not be located for 9 of the 30 individuals in our sample.


























Internet Protocol (IP) Addresses

We performed a specialist review over LSBU's external infrastructure. This review identified six recommendations required to mitigate the risk of an external malicious attack. Our work found that LSBU is running unsupported and outdated software on services visible over the internet; this exposes the infrastructure to attacks and could potentially compromise those services.

Continuous Auditing: Key Financial Systems - Period One – 2016/17

There has been a decline in performance this period. Untimely preparation and authorisation of reconciliations is a recurring theme, affecting Payroll and General Ledger. We have also continued to see exceptions affecting starter and leaver documentation within Payroll, which was either missing or has not been authorised on a timely basis.

Our ratings are based on the number and severity of findings noted for controls tested as part of the programme. This does not consider control design issues – these are individually risk rated. Please see table overleaf.

System / Rating	P1 2016/17	P2 2015/16	P1 2015/16	P3 2014/15	Trend
Payroll	 Amber	 Amber	 Green	 Green	
Accounts Payable	 Green	 Green	 Green	 Green	
Accounts Receivable	 Green	 Green	 Green	 Green	
Cash	 Green	 Green	 Green	 Amber	
General Ledger	 Amber	 Green	 Green	 Green	

Appendix 1 – Plan Progress

The below table outlines the progress against the 2015/16 Internal Audit Plan:

Days	ToR	Field work start	Exit Meeting	Final Report	Report Classification	Total findings	Ratings				
							Critical	High	Medium	Low	Advisory
Quarter 1: August 2015 – October 2015											
Continuous Auditing: Key Financial Systems - May 2015 to July 2015											
15 (15)	06/08/2014	17/08/2015	21/08/2015	08/09/2015	N/A	-	-	-	-	-	-
Quarter 2: November 2015 – January 2016											
Management Information: Data Quality											
10 (10)	21/01/2016	08/02/2016	17/02/2016	11/05/2016	Medium	5	-	-	4	1	-
Continuous Auditing: Student Data - August 2015 to October 2015											
12 (12)	13/11/2015	16/11/2015	27/11/2015	18/01/2016	N/A	-	-	-	-	-	-
HR System Implementation – Deferred to 2016/17											
2 (2)	06/01/2016	-	-	-	N/A	-	-	-	-	-	-
Research and Enterprise Contracts											
10 (10)	22/01/2016	25/01/2016	09/02/2016	15/04/2016	Medium	5	-	-	5	-	-
Quarter 3: February 2016 – April 2016											
Continuous Auditing: Key Financial Systems - August 2015 to December 2015											
16 (16)	17/12/2015	19/01/2016	05/04/2016	11/05/2016	N/A	-	-	-	-	-	-
Continuous Auditing : Student Data - November 2015 to March 2016											
13 (13)	14/04/2016	18/04/2016	29/04/2016	01/06/2016	N/A	-	-	-	-	-	-
Quarter 4: May 2016 – July 2016											
Risk Management											
5 (5)	09/05/2016	11/07/2016	16/08/2016	09/09/2016	Low	4	-	-	1	-	2
Prevent (Additional Review)											
10 (10)	09/05/2016	16/05/2016	28/06/2016	05/08/2016	Low	4	-	-	2	-	2
Information Security											
10 (10)	21/07/2016	01/08/2016	23/08/2016	13/09/2016	High	3	-	3	-	-	-
Other											
20 (20)	Planning, contract management, reporting, value for money and follow up										
Total	123 (123)										





The below table outlines the progress against the 2016/17 Internal Audit Plan:

Days	ToR	Field work start	Exit Meeting	Final Report	Report Classification	Total findings	Ratings				
							Critical	High	Medium	Low	Advisory
Quarter 1: August 2016 – October 2016											
Continuous Auditing: Key Financial Systems – January 2016 to July 2016											
13 (15)	19/08/2016	22/08/2016	05/09/2016	15/09/2016	N/A	-	-	-	-	-	
HEFCE 5 Year Review											
5 (0)											
HR System Implementation											
9 (1)											
Quarter 2: November 2016 – January 2017											
Placements											
8 (0)											
Continuous Auditing: Student Data – April 2016 to October 2016											
15 (0)					N/A	-	-	-	-	-	
Quarter 3: February 2017 – April 2017											
Continuous Auditing: Key Financial Systems - August 2016 to December 2016											
12 (0)					N/A	-	-	-	-	-	
Continuous Auditing : Student Data - November 2016 to March 2017											
15 (0)					N/A	-	-	-	-	-	
Apprenticeships											
7 (0)											
IT audit											
10 (0)											
Quarter 4: May 2017 – July 2017											
Risk Management											
5 (0)											
Contract Management and Spend Activity											
10(0)											
Other											
18 (5)	Planning, contract management, reporting, value for money and follow up										
Total	127 (21)										

Appendix 2 – Follow Up

Implemented

Review	Agreed action	Risk rating	Original due date	Status
Office of the Independent Adjudicator (OIA) 2013/14	Appeals LSBU are moving the system to an electronic workflow process which will be piloted during 2013/14 and fully implemented for the next main appeals cycle.	● Advisory	31/08/2014 30/09/2015 30/05/2016	The electronic system was discussed but not implemented. A new three stage appeals process has now been introduced by the registry team, and this is having a positive impact on the numbers of internal complaints commenced by students. Fewer internal complaints is having a positive impact on the numbers of OIA complaints.
Risk Management 2014/15	Risk Strategy Produce revised Risk Strategy addressing the issues identified including a section linking the Strategy to the latest business planning process.	● Low	30/11/2015 30/06/2016	The Risk Strategy has been revised to include a section linking the Strategy to the business planning process.
Risk Management 2014/15	Organisational Risks Implement updated 4-Risk platform, with new risk review functionality.	● Medium	31/12/2015 30/06/2016	The 4-Risk platform has been implemented. This includes the risk review functionality.
Risk Management 2014/15	Organisational Risks 2.2 Ensure the revised Risk Strategy and related training material explains the nature of risk and links to objectives more explicitly.	● Medium	30/11/2015 30/06/2016	The Risk Strategy has been updated and reviewed by the Strategic Risk Review group. The Strategy includes an explanation of the nature of risk and also links explicitly to LSBU's objectives.

Risk Management 2014/15	Organisational Risks 2.3 Deliver training to all risk owners on the updated 4-Risk system.	 Medium	31/03/2016 31/07/2016	Training has been provided to the majority of staff members. The dates for the remaining staff members have been arranged.
Risk Management 2014/15	Risk Review 3.1 We will update the Risk Strategy so it is consistent with our new processes.	 Low	30/11/2015 30/06/2016	The Risk Strategy has been updated.
Change Portfolio	Stakeholder Engagement During Project Approval Process Effective stakeholder management will be built into the LSBU project management approach. Initial engagement will be ensured through planned development of the business case process: a 'greenlight' stage is being proposed to Executive in October 2015, which ensures that opportunities identified and shared with all relevant stakeholders before business cases are developed. Business owners, stakeholders and support groups will then be involved throughout development. This will also support the pipeline approach, tracking prospects (opportunities) and projects, recently instituted in key teams including ICT and Research & Enterprise.	 Medium	30/11/2015 31/07/2016	A revised investment appraisal process has been prepared which captures the business case process. This process shall be ready for the the 2017/18 planning and investment cycle.
Change Portfolio	Resource Identification and Justification Business cases for technical projects now reflect business-as-usual and additional resources required, identifying true project costs and enabling a full cost-benefit analysis. Alongside the development of benefits identification, this approach will be built into the business case process for development projects across LSBU.	 Medium	30/11/2015 31/07/2016	A revised investment appraisal process has been prepared which captures the business case process. This process shall be ready for the the 2017/18 planning and investment cycle.

Research & Enterprise Contracts	<p>Research Contracts Compliance Monitoring</p> <p>We will update the Research Handbook to include roles and responsibilities for monitoring compliance with research contract terms and conditions.</p> <p>We will introduce a checklist for each research project to enable central monitoring of compliance with terms and conditions and progress against key milestones and deliverables. This will be completed by the Project Lead and uploaded onto Sharepoint to provide central oversight of all research contracts.</p> <p>We will introduce a formal 'kick-off' meeting for key Central Research Services and project staff to discuss key terms and conditions, key milestones and roles and responsibilities.</p>	<p>●</p> <p>Medium</p>	31/08/2016	<p>The updated Research Handbook has been drafted, this is expected to be finalised and issued to staff in September 2016. This was delayed as the project expanded beyond the recommendations raised by Internal Audit to capture all types of funded projects. We have reviewed the draft Handbook and verified that roles and responsibilities for monitoring compliance with research contracts terms and conditions have been outlined.</p> <p>The checklist concept has been developed into the Action Log that maps all research project key Terms and Conditions as well as planned and achieved dates for deliverables. The Action Log must be used by all research projects from 1st August 2016. The Action Log and Research Handbook states that a kick-off meeting is required.</p>
Research & Enterprise Contracts	<p>Research Contract Document Retention</p> <p>The Research Handbook will be updated to include:</p> <ul style="list-style-type: none"> • The documents which need to be retained for each research project; • The length of time key documents need to be retained; • The location and format (electronic/ hard-copy) documentation should be stored and; • Roles and responsibilities for retaining documentation. <p>The updated Research Handbook will be shared with all staff involved with Research Contracts.</p>	<p>●</p> <p>Medium</p>	31/08/2016	As outlined above, the Research Handbook is currently a draft document, expected to be published in September 2016. The draft Handbook includes a link to the policy on the retention of research and enterprise documents.
Research & Enterprise Contracts	<p>Finance Checks</p> <p>The eligibility check completed by the Finance team will be formalised and documented in the Research Handbook to ensure there is a consistent and robust process for all grant claims submitted.</p> <p>We will retain evidence of these checks.</p>	<p>●</p> <p>Medium</p>	31/08/2016	The Finance Team has developed an eligibility checklist for use on all research projects, this is available on the Finance Team's shared drive. The checklist is held separately from the Research Handbook as this is not relevant to Academics who are the target audience for the Handbook.

Research & Enterprise Contracts	<p>Research Contracts Expenditure Records</p> <p>The check completed by Finance will be formalised and documented in the Research Handbook to ensure there is a consistent process for all expenses claimed against research contracts.</p> <p>We will retain evidence of these checks.</p>	<p>●</p> <p>Medium</p>	31/08/2016	The Finance Team has developed guidance explaining the checks which need to occur on all research expenses. This document is held separately from the Research Handbook as this is not relevant to Academics who are the target audience for the Handbook.
Research & Enterprise Contracts	<p>Research Contracts Timesheet Controls</p> <p>We will introduce an approval process for timesheets claimed against research projects.</p> <p>The roles and responsibilities for the Finance Team will be outlined in the Research Handbook.</p>	<p>●</p> <p>Medium</p>	31/08/2016	<p>The Finance Team has developed guidance outlining the process for completing and approving a timesheet.</p> <p>The roles and responsibilities for the Finance Team are summarised in the Research Handbook.</p>

In progress

<i>Review</i>	<i>Agreed Action</i>	<i>Risk Rating</i>	<i>Original due date</i>	<i>Revised due date</i>	<i>Status</i>
Change Portfolio	<p>Portfolio Scope and Remit</p> <p>The role of portfolio management is clear – to provide oversight and support to development (or transformational) projects. Roles and accountabilities will not be developed further at this level. Activity is focussed on:</p> <ul style="list-style-type: none"> Establishing a best-in-class project management approach, detailing roles, accountabilities and controls on development projects across LSBU – building on the best practice approach recently introduced in ICT and existing practice across the university Benefits approach, stakeholder engagement process, and resource management approach (detailed against relevant findings, further in this document) Implementation of a 12-month project review process, including lessons learnt process. This 	<p>●</p> <p>Medium</p>	30/11/2015 31/07/2016	31/01/2017	<p>An adapted project management methodology for business change projects is still in development. This on hold pending recruitment of Deputy Director, Innovation & Transformation.</p> <p>12-month reviews of closed projects are still planned, however none have been conducted since the Audit report was issued.</p>

	is planned for projects delivered within the Change Programme, and will be detailed, with clear roles, responsibilities and outputs, in the LSBU project management approach.				
Change Portfolio	<p>Benefits Management</p> <p>Guidance for identifying project benefits: Alongside the implementation of the LSBU project management approach, a strategy and guidance for the definition, identification and specification of benefits is in development. This will support the creation and approval of business cases for investment.</p> <p>Reporting: benefits monitoring has now been built into monthly project reports, and an online reporting process is in development.</p> <p>Project closedown reports: benefits realisation: Within the 12-month project review process (noted against the previous finding), all identified benefits will be assessed to ensure they have been delivered or are on track. Guidance and oversight will ensure a consistent approach across LSBU projects.</p>	<p>●</p> <p>Medium</p>	30/11/2015	31/07/2016	<p>Guidance on benefits has not been completed. This shall be developed following the development of the project management methodology and business case approach which has been delayed pending recruitment of Deputy Director, Innovation & Transformation.</p> <p>The online reporting system has been implemented.</p>

Appendix 3 – Recent PwC Publications

As part of our regular reporting to you, we plan to keep you up to date with the emerging thought leadership we publish. The PwC PSRC produces a range of research and is a leading centre for insights, opinion and research on best practice in government and the public sector.

We are happy to provide full electronic or hard copy versions of these documents at your request.

All publications can be read in full at www.psrc.pwc.com/.

HE People Matters

In an increasingly competitive higher education market, the people agenda has become ever more significant. Universities are continually refining their approaches and procedures to attract, retain and develop a productive and fulfilled workforce. This special edition of HE Matters reflects on several of the fundamental people challenges universities are facing, now and in the future.

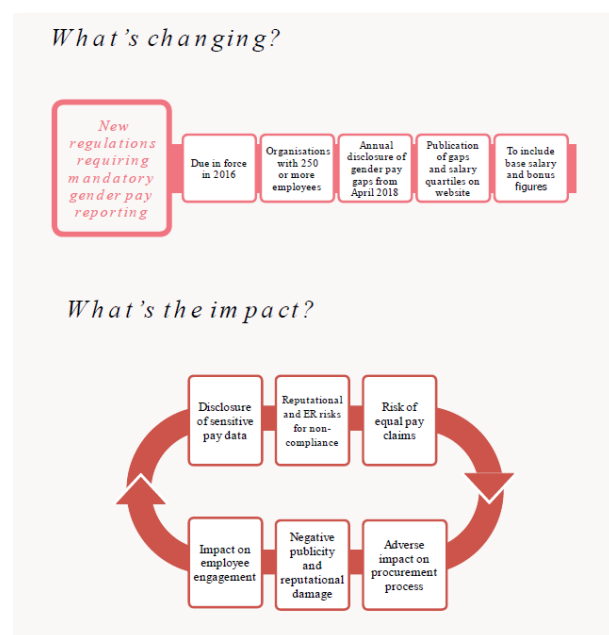
<http://www.pwc.co.uk/industries/government-public-sector/education/he-matters.html>



The following research has been issued to LSBU via email in the last quarter. Please contact us if you would like additional copies of these documents

Gender Pay Gap Reporting

New Gender Pay reporting regulations are coming into effect. The first disclosures required will be based on the pay period containing 30 April 2017 (so for monthly paid employees this would be the April 2017 pay period). Employers then have to analyse the data and publish results within a year. Going forward, disclosure will be required on an annual cycle based on pay periods containing 30 April.

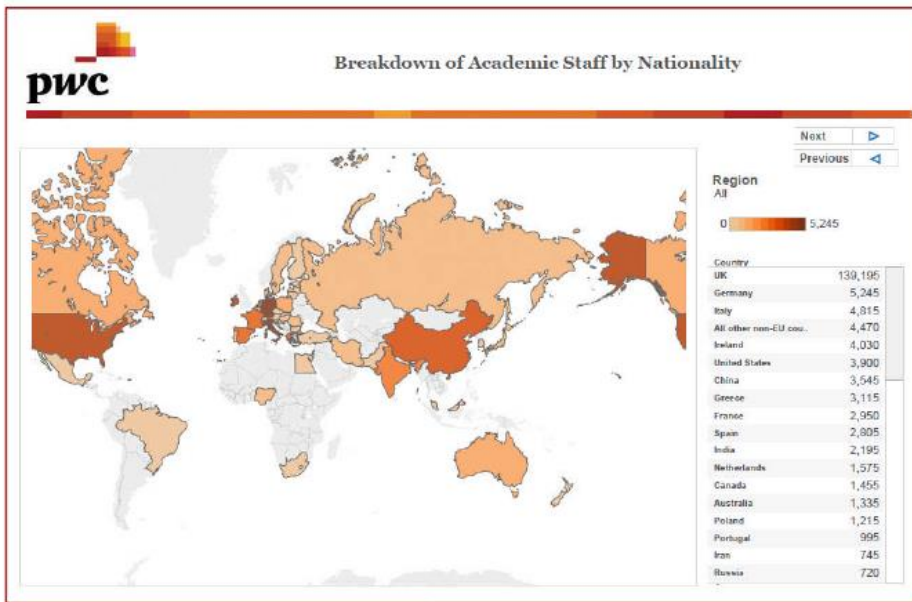


Brexit in HE

Our teams have put together a listing of PwC expertise available for Brexit concerns in a range of different areas. Please do not hesitate to contact us if you have queries or concerns in any of these areas.

Higher Education Implication	PwC Contact
<p>Immigration status of current and future staff and students Most universities currently have many employees and students from the EU. They will be wanting to re-assure those people of their current status, and how that may change.</p> <p>They will also be considering how the future framework for immigration will affect their ability to recruit staff and students, influencing talent management plans.</p>	<p>Immigration in higher education Julia Onslow-Cole (PwC Legal) Tel: 0207 212 6017 Email: julia.onslow-cole@pwclegal.co.uk</p> <p>Global mobility/talent management Marie Green (HR Tax) Tel: 0207 212 5591 Email: marie.green@uk.pwc.com</p>
<p>External finance Many universities either have invested in their estates and IT recently, or are planning to. Much of this is being funded externally using bank or bond finance. They will therefore be considering how Brexit may affect the future availability of finance for the sector.</p>	<p>External funding in higher education Daniel Earle (Corporate Finance) Tel: 0207 212 2536 Email: daniel.b.earle@uk.pwc.com</p>
<p>Strategic Planning Many university strategic plans look for growth (in terms of domestic and international students, and research), and Brexit may affect not only international student demand and EU research funding over time but also the competitive intensity for domestic students. Universities may therefore wish to re-assess their plans in the light of the Leave vote, or at least develop alternative scenarios to aid future planning.</p>	<p>Higher education strategy Ian Koxvold (Transaction Services) Tel: 0207 804 1592 Email: ian.koxvold@uk.pwc.com</p> <p>Financial planning Karen Dukes (BRS) Tel: 0207 804 4131 Email: karen.dukes@uk.pwc.com</p> <p>Ian Roberts (Risk Assurance) Tel: 0113 289 4066 Email: ian.d.roberts@uk.pwc.com</p>
<p>Exit Process Universities will be seeking to understand how the process for developing exit plans will work, and what they may expect when.</p>	<p>EU Referendum Alex Henderson Tel: 0207 213 4974 Email: alex.d.henderson@uk.pwc.com</p>
<p>Higher Apprenticeships and Skills Many universities are considering a future new market in providing higher apprenticeships, or in taking on further education and skills provision through acquisitions of further education/skills providers. The European Social Fund has been one source of skills funding in the UK. The Leave vote may create uncertainty over these plans.</p>	<p>Skills Chris Kirk (Consulting) Tel: 0207 213 3275 christopher.j.kirk@uk.pwc.com</p> <p>Michael Kane (Consulting) Tel: 02890 415 303 Email: michael.kane@uk.pwc.com</p> <p>Peter Norriss (Consulting) Tel: 0114 259 8287 Email: peter.norriss@strategyand.uk</p>
<p>Operational Matters Many other operational areas are affected by current EU regulations or by the implications of the Leave vote. Some of the more common ones include:</p> <ul style="list-style-type: none"> • Indirect tax, where much of the existing statute derives from EU regulation; • Employment law and HR taxes, where again much of the existing statute derives from EU regulation. • Pensions, many university pension funds are already under strain; a fall-off in investment performance will add pressure for change. 	<p>Richard Wallace (Indirect Tax) Tel: 02380 835 380 richard.e.wallace@uk.pwc.com</p> <p>Marie Green (HR Tax) Tel: 0207 212 5591 Email: marie.green@uk.pwc.com</p> <p>Pete Sparshott (Pensions) Tel: 020 721 24165 Email: peter.x.sparshott@uk.pwc.com</p>

Review of HESA data



Our review of data from HESA highlights that the UK higher education sector is highly reliant on overseas talent especially from the EU, the USA, China and India. PwC has a strong HE presence in all of the countries listed, placing us ideally to support universities wishing to employ individuals from these countries.



In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), London South Bank University is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, London South Bank University discloses any this document 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.

This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

	CONFIDENTIAL
Paper title:	Continuous Audit Report into Data Security
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Ian Mehrtens – Chief Operating Officer
Purpose:	To provide Committee with the results of the review into Data and Information Security.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This report relates to the reputation and compliance risk types expressed within the Risk Appetite, and relates mainly to the Resources & Infrastructure goal within the Strategy.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

This 15/16 internal audit survey follows on from a previous survey completed as part of the 14/15 audit plan,

This report is classified as high risk, and has 2 high, and 1 medium, findings (*pages 7 – 12*). These relate to the encryption of USB devices and laptops and other mobile devices, timely updates to user account permissions, and access control for physical locations with IT assets.

The report is accompanied by an External Infrastructure Vulnerability Assessment. This was completed by a 3rd party accessing current services and infrastructure externally exposed over the internet. The detailed technical findings are provided on pages 6 - 13.

- The Committee is requested to note and consider the report and its findings. The Head of Information Security will attend Committee to discuss matters in more detail.

Internal Audit Report 2015/2016

Data Security

*London South Bank
University*

September 2016

Final

▶ Click to launch


Page 30

Contents

Executive summary

1 

Background and scope

2 

Findings

Page 31 **3** 

Appendices

- A. Basis of our classifications
- B. Terms of reference
- C. Limitations and responsibilities

Distribution list

For action: Ian Mehrrens - Chief Operating Officer
Craig Girvan - Head of Information Security

For information: Richard Flatman - Chief Financial Officer
John Baker - Corporate and Business Planning Manager
Audit Committee



Executive summary (1 of 2)

Report classification

High Risk



Trend



Performance is consistent with the 2014/15 review.

Total number of findings

	Critical	High	Medium	Low	Advisory
Control design	0	2	0	0	0
Operating effectiveness	0	0	1	0	0
Total	0	2	1	0	0



Summary of findings

London South Bank University's (LSBU's) IT landscape has undergone a period of rapid change. While our risk rating is consistent with prior year, we recognise that a significant amount of work has been done to update and rationalise the logical and physical security controls in place. This includes linking the HR system with IT access so that leavers have their Active Directory (AD) accounts disabled automatically and the ongoing iTrent project which will allow an audit trail of all staff changes to staff access levels. Despite these improvements, a number of issues remain. We identified two *high risk* findings during our testing of user administration and logical security. A number of these findings were also identified in the 2014/15 Data Security internal audit.

Logical Security (finding #1)

We tested to confirm that controls and processes have been established to ensure that logical security settings are appropriate and applied consistently across the LSBU IT environment. We found:

- Unencrypted USB's can be used to extract data from the LSBU's systems.
- Contrary to the Mobile Devices Policy, users are able to 'opt out' of encrypting devices.
- Desktops aren't encrypted unless this is specifically requested.
- We were unable to obtain a complete listing of laptops held by the LSBU as a central list is not maintained. The listing that we did obtain showed that 77 of the 398 laptops known to the LSBU (19%) were not encrypted.
- The password parameters applied to Active Directory (AD) accounts differs to the Account Management policy.
- Laptops communicate with the network in order to update the encryption on the laptop. We identified that 356 of the 398 laptops listed (89%) had not communicated with the network for over 100 days.

Executive Summary (2 of 2)



User Administration (finding #2)

We reviewed the processes in place around user administration to ensure that there are appropriate controls for set up, modification and removal of user accounts. We found:

- ICT are not notified when an individual has moved within LSBU and we were unable to obtain a listing of changes made to user access. We understand from management that it is likely that members of staff who've changed position retain access to data that they are no longer permitted to see.
- For our sample of 30 leavers tested, four leavers AD accounts were still active at the date of fieldwork.

We identified one *medium risk* finding:

Physical Security (finding #3)

- We reviewed the procedures and controls in place to ensure the physical security of LSBU's buildings and associated IT assets. We visited five ICT storage areas to confirm that these were only accessible to specific ICT staff and found two of the buildings had active ICT network equipment that was not appropriately restricted.
- We tested the controls in place for providing security passes to staff. Forms could not be located for nine of the 30 individuals in our sample.

Internet Protocol (IP) Addresses: Our work over IP addresses has been completed by a specialist PwC team and summarised in a separate report. The results from this testing are not included in the findings outlined above.



Background and scope (1 of 2)



Background and audit objectives

IT controls are integral to protecting an organisation’s information data and assets (physical and intellectual).

Our 2014/15 review of IT controls was classified as high risk and identified several issues arising from weak logical and physical controls and inadequate authorisation processes for user administration.

LSBU uses IP addresses to connect devices within the network. IP addresses allow information to be shared across devices. Strong controls over the use of IP addresses are required to ensure confidential information is managed appropriately.

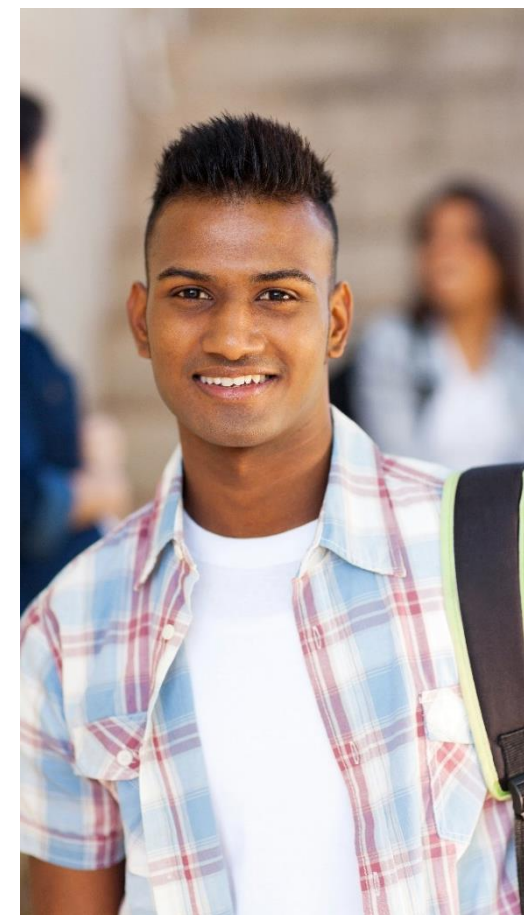
The purpose of this review was to assess the design and operating effectiveness of controls over data security by reviewing progress made in high risk areas and to consider the controls in place over IP addresses. Our work on IP addresses is contained in a separate report.

Our work touched upon the following areas of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management
10	x		x	x	x

x = area of primary focus

x = possible area of secondary focus



Background and scope (2 of 2)



Scope

We included the following sub-processes and related control objectives in this review:

Sub-process	Objectives	Work to be completed
User Administration (Starters, Movers and Leavers)	Controls are established to ensure that user accounts are appropriately authorised prior to creation, accounts are modified or removed when employees change roles or leave LSBU.	<ul style="list-style-type: none"> We will test a sample of starters, movers and leavers on LSBU's systems to assess whether access is appropriate to their roles.
Physical Security Management	Controls are established to ensure the physical security of LSBU's buildings and associated IT assets.	<ul style="list-style-type: none"> We will review physical access controls to LSBU's IT assets, including workstations, portable devices and network equipment.
Logical Security Management	Controls are established to ensure that logical security settings are appropriate and applied consistently across LSBU's IT environment to prevent data loss, unauthorised access, or theft.	<ul style="list-style-type: none"> We will test key controls in place to ensure logical security settings are appropriate and applied across the IT environment.
IP addresses	Controls are established to ensure that information retained within LSBU's network is secure.	<ul style="list-style-type: none"> We will test a sample of IP addresses to assess whether confidential data held within LSBU's network is appropriately protected.

Limitations of scope

Our review was focussed on controls around LSBU's staff accounts and infrastructure and did not assess the controls over student accounts or IT infrastructure, except where the same controls exist for both staff and students.

We performed follow up work of high risk findings throughout the year, this work was not repeated in this review. This audit focussed on substantive testing of controls implemented to confirm they are operating as designed.

Logical Security

Control design & operating effectiveness

1

Page 36

Finding rating

Rating

High

Findings

We tested to confirm that controls and processes have been established to ensure that logical security settings are appropriate and applied consistently across LSBU's IT environment.

We identified the following control design exceptions:

- Unencrypted USBs can be used on the network to remove data. All information that is transferred onto an unencrypted USB is then encrypted but LSBU is unable to determine what information has been taken off the system. This issue was also raised in our 2014/15 report.
- It is not mandatory for mobile devices to be encrypted - users have the ability to 'opt out' through a disclaimer form. While this is not widely done (only three devices were found to be 'opted out'), it is not in line with the Mobile Device Policy. This finding was also raised in the 2014/15 review where seven devices had 'opted out'. The Mobile Device Policy has not been updated since 24/04/2013.
- Desktop devices are not encrypted except in situations where users are specifically identified as dealing with sensitive data. This issue was also raised in our 2014/15 report.
- We requested a report of laptops held by LSBU to determine whether they were appropriately encrypted. From discussion with management, we understand that it is not possible to obtain a complete listing of laptops and therefore establish the number of unencrypted devices.

As well as the control design findings outlined above, we also identified the following operating effectiveness findings:

- The password parameters applied in AD differs to the Account Management policy. The Account Management policy states user accounts should be locked out after five incorrect attempts. The AD password parameters are set up to lock accounts after six failed attempts.
- We obtained a listing of laptops held LSBU. From discussions with management we understand that this listing is likely to be incomplete as there is no centrally held register of laptops. Of the 398 laptops known to LSBU, 77 (19%) were not encrypted. This issue was also raised in our 2014/15 review where 43 of the 252 laptops known to LSBU (17%) were not encrypted.
- Laptops communicate with the network in order to update the encryption on the laptop. We identified that 356 of the 398 laptops listed (89%) had not communicated with the network for over 100 days.

Logical Security

Control design & operating effectiveness

Continued

1

Page 37

Finding rating

Rating

High

Implications

Inadequate or inconsistent logical security may lead to an increased risk of unauthorised access to sensitive data and transactions with subsequent risk of information abuse and / or fraud, and adverse impact upon LSBU's reputation.

Action plan

- We are not able to technically restrict unencrypted USB devices across the whole organisation as this would have a negative impact on teaching and learning, as well as on our disabled students. Instead we will begin deploying encrypted USBs to all staff that request them, and enforcing by policy; that all members of staff must use LSBU provided encrypted USBs whenever transporting any data away from their machines.
- We have not been accepting 'opt outs' for encryption policies since July 2015, we will no longer be accepting 'opt outs' for any encryption related policy. This messaging will be reinforced to our helpdesks during September.
- We have undertaken a cost benefit analysis of known desktop machines across the organisation. We have identified that public machines hold no accessible sensitive information therefore can be viewed as low risk. As a department we have decided that only sensitive devices will be encrypted.
- We recently (August 2016) implemented a system (System Centre Configuration Manager) capable of cataloguing and tracking machines across our network. This system will help to address historic tracking issues for laptops and other mobile devices. We are expecting this system to reach maturity by the end of 2016. In addition we are exploring options to restrict access to staff areas of the network to only allow registered and tracked devices (Network Access Control system) during the 16/17 academic year.
- The password parameters applied in AD are a known issue related to a deprecated system that has been decommissioned, a change request has been submitted as of 07/09/2016 to have the technical password policy parameters changed.
- We will review the listing of incomplete encryptions and remind users to ensure that these are up-to-date so they are actively encrypted. As above, this work will be covered as part of our SCCM database.

Responsible person/title:

Craig Girvan, Head of Information Security

Target date:

31/01/2017

Reference number:

1

User Administration

Control design & operating effectiveness

2

Page 38

Finding rating

Rating

High

Findings

We reviewed the processes in place around user administration to ensure that there are appropriate controls around set up, modification and removal of user accounts.

We identified the following control design findings:

- ICT are not notified when an individual has moved within LSBU. LSBU is unable to generate a report showing movers within the University. From discussion with management, we understand that access rights to shared data is additive, which means that when a member of staff moves intra-departmentally the user's existing access will be retained. This finding was included in the 2014/15 Data Security report.
- We also identified during our fieldwork that there are a number of staff who have more than one AD account. There are two reasons for multiple accounts:
 - A staff member is also a student requiring two separate accounts
 - Administrative access requires a different account.

The staff/student separate accounts are not noted as an issue as this is the way that the system is structured and staff AD access is terminated as soon as employment ceases. The secondary administrative accounts are also acceptable if administrative access is reviewed on a regular basis. We noted that while Domain Administrators are reviewed biannually, lower level administrative access is not currently reviewed.

In addition we identified the following operating effectiveness findings:

- Four of the 30 leavers sampled, still had active AD accounts at the date of fieldwork. In the 2014/15 Data Security report, we found that three of the 30 leavers tested still had active AD access despite leaving LSBU.

User Administration

Control design & operating effectiveness

Continued

2

Page 39

Finding rating

Rating

High

Implications

- Inadequate control over the user accounts may increase the risk of unauthorised access to sensitive records and data.
- If leavers are not removed from the system in a timely manner, LSBU increases the risk that inappropriate access or loss of data will occur, causing system outages or potential reputational damage.

Action plan

- The dual accounts are by design as there are technical administrators that only undertake authoritative actions on the systems by invoking their '1' account. No administrator is allowed to log on 'interactively' with their 1 account, it is only used for privilege escalation as and when that is required. In order to mitigate the risk that administrative accounts are retained after they are no longer needed, we have undertaken quarterly reviews of all '1' accounts across the organisation, the first of which was instituted on 05/09/16.
- The implementation of the new HR iTrent system will enable an audit trail of all changes to staff access.

Responsible person/title:

Craig Girvan, Head of Information Security

Target date:

31/01/2017

Reference number:

2

Physical Security

Operating effectiveness

3

Page 40

Finding rating

Rating

Medium

Findings

We reviewed the procedures and controls in place to ensure the physical security of LSBU's buildings and associated IT assets. We found:

- All ICT storage areas should be key card controlled and only be accessible to specific ICT staff (general staff passes do not grant access to these ICT storage areas). We selected five buildings to confirm whether physical ICT assets were securely stored. Of the five buildings tested, two were found to have servers accessible to anyone in the building.
 - i. The K2 building had one exception which was a network infrastructure cupboard that was accessible on a general staff pass.
 - ii. The Borough Road building had two exceptions where network infrastructure was accessible on a general staff pass.

In the 2014/15 Data Security review, the same finding was identified with inappropriate physical controls identified for two of five buildings sampled.

- Two items included in the IT assets listing could not be located during the audit. We understand from management that these two assets no longer exist. These were the Mini-cabs at Perry Library and the K2 Building.
- We tested the controls in place for providing security passes to staff. Forms could not be located for 9 of the 30 individuals in our sample.

Physical Security

Operating effectiveness

Continued

3

Page 4

Finding rating

Rating

Medium

Implications

Inadequate control over physical security may result in the loss or theft of physical IT assets as well as the loss or theft of data, resulting in potential financial or reputational damage for LSBU.

Action plan

- We will continue to review the physical security controls in place for all IT assets held by LSBU. The physical security weaknesses addressed in this document have been identified and remediated to an acceptable level given environmental constraints.
- We are currently going through a datacentre move, in which we have some assets moving to the DC in Keyworth, as well as moving some assets from physical machines to virtual. As part of that project's closure, we will review and reconcile the IT Asset register.
- The security controls in question need to be reviewed more thoroughly before we take steps to remediate these controls. It is not clear that the forms in question were unavailable due to failings in the process.

Responsible person/title:

Craig Girvan, Head of Information Security

Target date:

31/01/2017

Reference number:

3

Appendices

Appendix A: Basis of our classifications

Individual finding ratings

Critical

A finding that could have a:

- **Critical** impact on operational performance resulting in inability to continue core activities for more than two days; or
- **Critical** monetary or financial statement impact £5m; or
- **Critical** breach in laws and regulations that could result in material fines or consequences over £500k; or
- **Critical** 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.

High

A finding that could have a:

- **Significant** impact on operational performance resulting in significant disruption to core activities; or
- **Significant** monetary or financial statement impact of £2m; or
- **Significant** breach in laws and regulations resulting in significant fines and consequences over £250k; or
- **Significant** impact on the reputation or brand of the organisation, resulting in unfavourable national media coverage.

Medium

A finding that could have a:

- **Moderate** impact on operational performance resulting in moderate disruption of core activities or significant disruption of discrete non-core activities; or
- **Moderate** monetary or financial statement impact of £1m; or
- **Moderate** breach in laws and regulations resulting in fines and consequences over £100k; or
- **Moderate** impact on the reputation or brand of the organisation, resulting in limited unfavourable media coverage.

Appendix A: Basis of our classifications

Individual finding ratings

Low

A finding that could have a:

- **Minor** impact on the organisation’s operational performance resulting in moderate disruption of discrete non-core activities; or
- **Minor** monetary or financial statement impact of £500k; or
- **Minor** breach in laws and regulations with limited consequences over £50k; or
- **Minor** impact on the reputation of the organisation, resulting in limited unfavourable media coverage restricted to the local press.

Advisory

A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Report classifications

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

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

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

Appendix B: Terms of reference

To: Ian Mehrtens – Chief Operating Officer

From: Justin Martin – Head of Internal Audit

Background and audit objectives



This review is being undertaken as part of the 2015/2016 internal audit plan approved by the Audit Committee.

Background and audit objectives

IT controls are integral to protecting an organisation’s information data and assets (physical and intellectual).

Our 2014/15 review of IT controls was classified as high risk and identified several issues arising from weak logical and physical controls and inadequate authorisation processes for user administration.

LSBU uses IP addresses to connect devices within the network. These IP addresses allow information to be shared across devices. Strong controls over the use of IP addresses are required to ensure confidential information is managed appropriately.

The purpose of this review is to assess the design and operating effectiveness of controls over data security by reviewing progress made in high risk areas and to consider the controls in place over IP addresses.

Our work touches upon the following areas of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management
10	x		x	x	x

x = area of primary focus

x = possible area of secondary focus

Audit scope and approach (1 of 2)

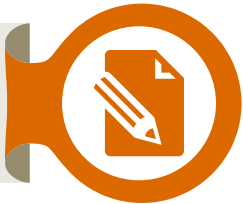


Scope

The sub-processes, related control objectives and key risk areas included in this review are:

Sub-process	Objectives	Work to be completed
User Administration (Starters, Movers and Leavers)	Controls are established to ensure that user accounts are appropriately authorised prior to creation, accounts are modified or removed when employees change roles or leave LSBU.	<ul style="list-style-type: none"> We will test a sample of starters, movers and leavers on LSBU systems to assess whether access is appropriate to their roles.
Physical Security Management	Controls are established to ensure the physical security of LSBU's buildings and associated IT assets.	<ul style="list-style-type: none"> We will review physical access controls to LSBU's IT assets, including workstations, portable devices and network equipment.
Logical Security Management	Controls are established to ensure that logical security settings are appropriate and applied consistently across the LSBU IT environment to prevent data loss, unauthorised access, or theft.	<ul style="list-style-type: none"> We test key controls in place to ensure logical security settings are appropriate and applied across the IT environment.
IP addresses	Controls are established to ensure that information retained within LSBU's network is secure. .	<ul style="list-style-type: none"> We will test a sample of IP addresses to assess whether confidential data held within LSBU's network is appropriately protected.

Audit scope and approach (2 of 2)



Limitations of scope

This review will focus on controls around LSBU’s staff accounts and infrastructure and will not assess the controls over student accounts or IT infrastructure, except where the same controls exist for both staff and students.

We have performed follow up work of high risk findings throughout the year. We will not repeat this work; this audit will focus performing substantive testing of controls implemented to confirm they are operating as designed.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the data security environment through discussions with key personnel, review of key documentation.
- Identify the key risks of the data security environment.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the key controls.



Internal audit team and key contacts



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@uk.pwc.com
Charlotte Bilsland	Engagement Senior Manager	07715 484 470 charlotte.bilsland@uk.pwc.com
Lucy Gresswell	Engagement Supervisor	07718 098 321 lucy.j.gresswell@uk.pwc.com
Joshua Wilson	Auditor	joshua.j.wilson@uk.pwc.com

Key contacts – London South Bank University

Name	Title	Contact details
Ian Mehrtens	Chief Operating Officer (Audit Sponsor)	020 7815 6804 ian.mehrtens@lsbu.ac.uk
Craig Girvan	Head of Information Security (Audit Contact)	0207 815 6588 girvanc@lsbu.ac.uk
Richard Flatman	Chief Financial Officer	0207 815 6301 richard.flatman@lsbu.ac.uk
John Baker	Corporate and Business Planning Manager	0207 815 6003 j.baker@lsbu.ac.uk



Timetable and information request



Timetable

Fieldwork start	25 July 2016
Fieldwork completed	5 August 2016
Draft report to client	12 August 2016
Response from client	17 August 2016
Final report to client	19 August 2016

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.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Please note that if the University requests the audit timing to be changed at short notice (2 weeks before fieldwork start) and the audit staff cannot be deployed to other client work, the University may still be charged for all/some of this time. PwC will make every effort to redeploy audit staff in such circumstances.

Information request

- Listing of Admin users
- Listing of starters, movers and leavers within the year
- A list of ICT storage areas
- A listing of IP addresses

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. 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.

Future periods

Our assessment of controls is for the period specified only. 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 changes; or
- The degree of compliance with policies and procedures may deteriorate.

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 endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we 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.

This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to the Memorandum of Assurance and Accountability (MMA) between Higher Education Funding Council for England (HEFCE) and institutions. 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.

In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), London South Bank University is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, London South Bank University discloses any this document 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.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

*External
Infrastructure
Vulnerability
Assessment*

Issue Date:
September 2016

London South Bank
University

Contents

1. Introduction	3
2. Executive Summary	4
3. Summary of Findings	5
4. Detailed Technical Findings	6
5. Appendix A: Document Control	14
6. Appendix B: Detailed Scope	15
7. Appendix C: Risk Ratings	18
8. Appendix D: Affected Hosts	22

1. Introduction

London South Bank University (LSBU) commissioned PricewaterhouseCoopers (PwC) to complete an independent vulnerability assessment of their external infrastructure. This assessment will feed into the Internal Audit review of LSBU's IT controls by assessing the risks and vulnerabilities relating to the IP's provided.

This report has been prepared for and only for London South Bank University in accordance with the terms of our engagement letter and Terms of Business dated 21/07/2016 and our Testing Authorisation Letter (TAL) dated 21/07/2016.

Summary of objectives

The external vulnerability assessment objective was to enable London South Bank University to understand the current IT security risk profile with the exposed services to the Internet and to provide recommendations to help reduce these risks. The assessment was designed to replicate the activities of a malicious external threat actor with the intention of gaining access to LSBU's business data and systems through exploiting vulnerabilities within the externally exposed services.

Summary of scope

The scope of our assessment includes an external vulnerability assessment only. Full details of the target systems in scope, together with specific limitations of the assessment are listed in Appendix B: Detailed Scope.

<i>Project title:</i>	External Infrastructure Vulnerability Assessment
<i>Project description:</i>	External Infrastructure Vulnerability Assessment
<i>Fieldwork dates:</i>	01 August – 05 August 2016
<i>PwC consultant testers:</i>	Holly Rostill

2. Executive Summary

Our assessment of the external infrastructure found that the root cause of vulnerabilities identified in this assessment were related to system configuration. These included encryption configuration weaknesses as well as unsupported software and missing patches.

A number of hosts were identified to be running unsupported software, these contain several vulnerabilities which are unlikely to be resolved as patches for these versions are no longer released. There were also missing patches identified on some of the supported software and these patches should be applied to fix any potential vulnerabilities on the hosts.

Unsupported software should be replaced with a matter of urgency. If these patches are not applied or the unsupported software is not replaced then an attacker could be able to exploit vulnerabilities to potentially compromise the servers and the data held on them, it may also provide a foothold onto the LSBU network.

In detail, the assessment identified six findings. Of these, we consider one finding to represent a critical risk, two a medium risk with the remainder representing low risks or provided for your information. A full breakdown of the findings has been provided in the graph below, broken down by root cause area.



Management Response

We are pleased to note the results of this exercise. It is reflective of our significant work over firewalls and updating of Microsoft 2003 across the estate. We will continue to address weaknesses as identified on an ongoing basis.

3. Summary of Findings

Below is a summary of the findings identified during the assessment ranked by risk rating. All findings are assessed by the testing team and rated according to our judgement. The ratings are intended as a guide to help you understand the priority of any remedial actions. A guide to the calculation of our risk ratings can be found in Appendix C: Risk Ratings.

You should review each rating in line with your own risk management framework and knowledge of your technical and business environment. This may result in you assigning different risk ratings to the ones highlighted in this report.

External Infrastructure Vulnerability Assessment

<i>Ref.</i>	<i>Risk</i>	<i>Finding</i>	<i>Hosts Affected</i>	<i>Recommendation</i>
EXT-01	Critical	Unsupported Software	136.148.38.121 136.148.38.156	Update Microsoft Windows Server 2003 and Phpbb 2.0.8 to supported versions.
EXT-02	Medium	Missing Patches	See Appendix D	Apply any necessary patches as a matter of urgency.
EXT-03	Medium	Encryption Weaknesses	See Appendix D	Self-signed or untrusted certificates should be replaced with legitimate certificates. Weak ciphers should be removed and replaced following best practise guidelines.
EXT-04	Low	Frameable Responses (Clickjacking)	See Appendix D	Anti-clickjacking headers should be implemented across all applications.
EXT-05	Info	Information Disclosure	See Appendix D	Disable or remove the software version information from server headers. Delete any default installation files available on the web server that are not required by the application.
EXT-06	Info	Closed Ports	See Appendix D	Reconfigure firewalls so that no responses are received from the host if the service is not receiving traffic.

4. Detailed Technical Findings

This section contains the full detail for each finding identified during the assessment, including a full description, associated risks and recommendations to help mitigate the risks.

External Infrastructure Vulnerability Assessment

EXT-01. Unsupported Software

Hosts:	Risk rating:	Critical
136.148.38.121 – Windows Server 2003	Impact:	9
136.148.38.156 – PhpBB 2.0.8	Ease:	10
	Root cause area:	System Configuration

Description

One host was identified to be running an unsupported operating system. The operating system was identified as Microsoft Windows Server 2003 (Microsoft IIS-6.0) and has been unsupported since July 2015. The version was identified from the server headers returned by the host.

Additionally, one host was using an unsupported forum package. The forum package was identified as PhpBB version 2.0.8 which was been unsupported since 2009 and has several critical vulnerabilities relating to it such as remote file inclusion. This was identified by browsing to the following URL;

<http://136.148.38.156/php4-cgiwrap/nonmedrx/phpBB>

Risk

The version of Microsoft IIS installed, IIS-6.0, is installed as part of Microsoft Windows Server 2003, it has been unsupported since July 2015. Due to it being unsupported, the vendor no longer supplies updates to Windows. If further security vulnerabilities are identified in the software, it could leave LSBU open to attack by malicious threat actors leveraging these unresolved security vulnerabilities.

Furthermore, the version of PhpBB installed, 2.0.8, has been unsupported since 2009 and has several critical vulnerabilities relating to it such as remote file inclusion. This vulnerability also has a known exploit which an attacker could easily run to output the contents of LSBU's files, execute code on the server or to commit a Denial of Service attack. This application seemed to involve prescription/medical data and so any data the attacker gathers could be extremely sensitive.

Recommendation

- Replace outdated operating systems with up to date and supported operating systems, upgrade installed software to the latest version and ensure updates are applied on a regular basis. At the time of the test the latest versions were;
 - Microsoft IIS 10.0, Windows Server 2016/ IIS 8, Windows Server 2012
 - PhpBB 3.2.0

EXT-02. Missing Patches

Hosts:	Risk rating:	Medium
See Appendix D	Impact:	7
	Ease:	5
	Root cause area:	System Configuration

Description

A number of missing patches were identified, some of which are rated as a high or critical risk. These include:

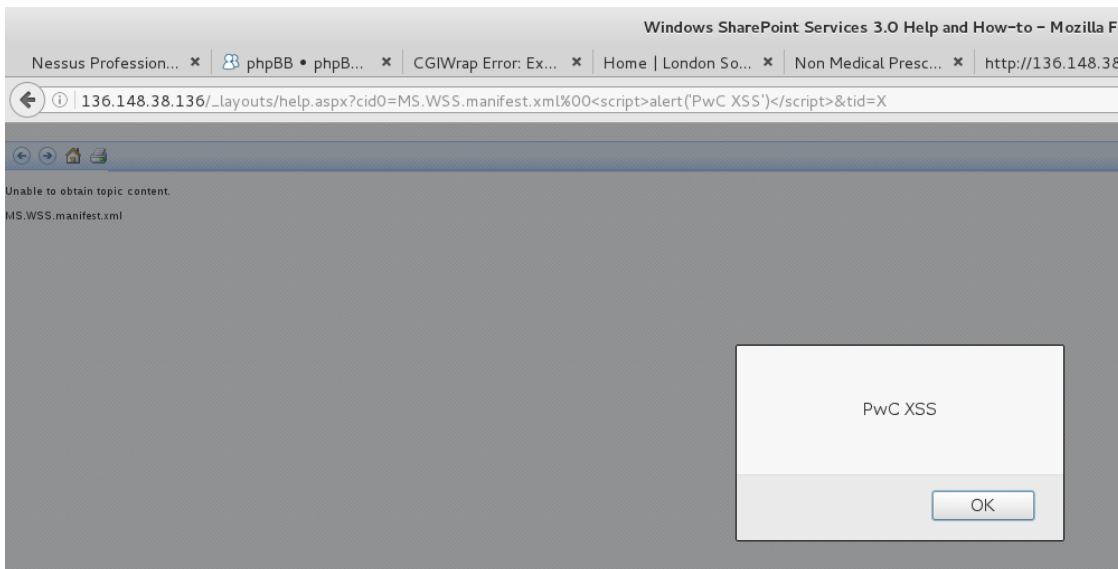
- Microsoft Sharepoint; and
- OpenSSL
- Apache

Risk

Vulnerabilities in the out-of-date software identified could enable an attacker to compromise an LSBU web server or carry out Denial of Service (DoS) attacks.

A missing patches for Microsoft Sharepoint included a Cross-site Scripting vulnerability, this could allow an attacker to execute malicious code on the application. This was done by browsing to the following URL and entering '<script>alert('PwCXSS')</script>' in the parameter as shown in the URL and screenshot below.

[http://136.148.38.136/_layouts/help.aspx?cid0=MS.WSS.manifest.xml%00<script>alert\('PwCXSS'\)</script>&tid=X](http://136.148.38.136/_layouts/help.aspx?cid0=MS.WSS.manifest.xml%00<script>alert('PwCXSS')</script>&tid=X)



NOTE: Linux distributions regularly backport security updates without changing the version number, therefore LSBU should perform further checks to determine whether appropriate patches have been applied.

Recommendation

- Apply any missing patches to software as a matter of urgency and updates are applied regularly in a timely manner. At the time of the test the latest versions were;
 - Sharepoint Server 2016
 - OpenSSL 1.0.2
 - Apache 2.4.23

EXT-03. Encryption Weaknesses

Hosts:	Risk rating:	Medium
<i>See Appendix D</i>	Impact:	7
	Ease:	3
	Root cause area:	System Configuration

Description

Secure Sockets Layer (SSL), or the more recent Transport Layer Security (TLS), is a protocol used to provide cryptographic protection to other network services. It can provide confidentiality and integrity of exchanged data and authentication of the communicating parties. SSL relies on certificates to provide authentication of the endpoints, which is the foundation on which the other cryptographic properties rely. Each certificate must be signed by a Certificate Authority (CA) known to both sides of the endpoint to have any effect.

Several issues with the way the SSL has been configured on both of the applications have been identified. This includes:

- Self-signed and untrusted certificates are presented by the application;
 - Support for the legacy SSL protocols; SSLv3 and SSLv2;
 - Vulnerable to 'POODLE'; and
 - Use of weak ciphers such as RC4.
-

Risk

Older versions of the TLS/SSL protocol have publically known security weaknesses. In some cases, these can permit an attacker, in a position to intercept network traffic, to downgrade the security level provided by the TLS service. This issue, together with support for weak ciphers, may permit an attacker to decrypt or modify information in transit between the application and its clients.

Using invalid or weak certificates can permit an attacker to impersonate the legitimate TLS protected service. Most applications will display a warning to the user when an incorrect certificate is received. However, if users are accustomed to accepting these warnings as the service uses an invalid certificate, they are likely to ignore any other warnings. This would allow the attacker to transparently decrypt and traffic sent between the user and the application and access any confidential information contained therein.

Carrying out attacks directly against weak ciphers would require the attacker to be able to access network traffic between the application and its clients, and a significant amount of computing resources. Most of the known attacks against older versions of TLS/SSL are theoretical and limited examples exist of successful real-world attacks.

Recommendation

- Configure a valid certificate on every service, this should be signed by a known Certificate Authority (CA) using a supported hashing algorithm (such as SHA256) and with the correct address of the system.
 - Disable weak ciphers such as RC4 and replace with best practice guidelines such as AES 128-256
 - Disable support for older versions of the TLS and SSL protocol, such as SSL v2 or SSL v3. Only the most recent version of TLS, version 1.2, should be supported. Note: that disabling older versions of TLS can prevent some legacy clients from connecting to the service.
-

EXT-04. Frameable Responses (Clickjacking)

Hosts:	Risk rating:	Low
<i>See Appendix D</i>	Impact:	6
	Ease:	3
	Root cause area:	System Configuration

Description

For a number of the hosts it was identified that application responses did not include security headers designed to prevent pages loading inside frames. This can permit an attack known as click-jacking. An attacker can craft a malicious website that includes a hidden frame containing the assessed applications. If they can induce a user to access the malicious website, the browser will interpret their actions, such as entering data and mouse clicks, as taking place in the target application. However, as the frame is hidden, the user will think they are interacting with the legitimate site.

Risk

A successful clickjacking attack could result in unauthorised activity being carried out within the application. This could include downloading malware to their machine or entering their user credentials into the fake site instead of the legitimate LSBU site.

Recommendation

- It is recommended that anti-click jacking headers be applied to all pages within all the applications tested. This can be done by adding the following features within the applications web server configuration file:
 - To prevent framing altogether use the following:
 - X-Frame-Options: Deny
 - To allow framing only by pages on the same origin as the response itself use the following:
 - X-Frame-Options: SAMEORIGIN
-

EXT-05. Information Disclosure

Hosts:	Risk rating:	Info
<i>See Appendix D</i>	Impact:	1
	Ease:	10
	Root cause area:	System Configuration

Description

All applications were found to disclose information in a number of ways, including:

- Default files;
- Browsable Web Directories
- Verbose Server Headers; and
- Verbose Error Messages;

These contained sensitive information about the application such as available pages, server names, version numbers and others.

Risk

The sources listed above provide more information related to the environment and underlying infrastructure to an attacker, using information allows them to gather information which may be used in an attack against the organisation. This could also enable an attacker to compromise servers by identifying version numbers and any vulnerabilities relating to that version.

Recommendation

- Remove unnecessary information, such as default files and server headers, from the users view.
-

EXT-06. Closed Ports

Hosts:	Risk rating:	Info
<i>See Appendix D</i>	Impact:	2
	Ease:	10
	Root cause area:	System Configuration

Description

It was identified that a large number of hosts had many closed ports including;

- Port 22
 - Port 993
 - Port 143
 - Port 8443
 - Port 443
 - Port 8080; and
 - Port 8000
-

Risk

When a 'closed status' is returned by a port query, even though the port is not accepting any packets, this still tells an attacker that this host exists. This could then lead to an attacker performing a Denial of Service (DOS) attack on this host or help to identify information relating to it.

Recommendation

- Reconfigure the firewall so that if a port is not accessible to a user the host returns nothing to any port queries.
-

5. Appendix A: Document Control

Author(s): Holly Rostill

Our reference: 160805

Document version information

<i>Date</i>	<i>Author</i>	<i>Version</i>	<i>Comment</i>
12/08/2016	Holly Rostill	0.1	Initial document
12/08/2016	Ryan Siu	0.2	QA review
12/08/2016	Ryan Siu	1.0	Engagement leader review

Distribution

<i>Name</i>	<i>Organisation</i>	<i>Copy #</i>
TVM Team	PwC	N/A
Lucy J Gresswell	PwC	N/A

6. Appendix B: Detailed Scope

PwC performed a vulnerability assessment on behalf of London South Bank University that comprised the following services:

External Infrastructure Vulnerability Assessment

An external vulnerability assessment designed to replicate the position of a malicious internal user with logical access to your networks. Intrusive testing was out of scope for this component.

The systems and networks in scope for this component are detailed below.

External Penetration Test	
Platform external IPs	
Hostname	IP address
my.lsbu.ac.uk	136.148.61.49
ict-helpdesk.lsbu.ac.uk	136.148.77.111
secure.lsbu.ac.uk	136.148.233.249
llr.lsbu.ac.uk	136.148.38.136
authoring.lsbu.ac.uk	136.148.61.45
hear.lsbu.ac.uk	136.148.39.51
alumni.lsbu.ac.uk	136.148.38.92
llrbookings.lsbu.ac.uk	136.148.38.80
apply-international.lsbu.ac.uk	136.148.38.236
blog.lsbu.ac.uk	136.148.38.157
sinope64.lsbu.ac.uk	136.148.38.156
danube.lsbu.ac.uk	136.148.38.132
apps.lsbu.ac.uk	136.148.38.126
clearing.lsbu.ac.uk	136.148.38.106
myweb.lsbu.ac.uk	136.148.38.164
wwwt.lsbu.ac.uk	136.148.36.116
phonebook.lsbu.ac.uk	136.148.38.102

eportfolio.lsbu.ac.uk	136.148.35.142
mail.lsbu.ac.uk	136.148.35.150
smtp.lsbu.ac.uk	136.148.76.95
register.lsbu.ac.uk	136.148.38.121
bus.lsbu.ac.uk	136.148.38.155
forge.lsbu.ac.uk	136.148.77.49
kxweb.lsbu.ac.uk	136.148.38.177
br-dns1.lsbu.ac.uk	136.148.108.21

General limitations

Technical security reviews seek only to expose weaknesses through specific and realistic testing from a predetermined scenario. It does not positively test all possible controls, or expose all possible control weaknesses. A detailed diagnostic review of all the individual components and related procedures is necessary to achieve this goal, which was beyond the scope of this assignment.

The assessment is a point-in-time snapshot. IT systems and threat profiles are constantly evolving and new vulnerabilities are discovered all the time. Therefore, it is possible that vulnerabilities exist, or will arise that have not been identified.

Our assessment is purely technical and we did not attempt to identify other issues, such as regulatory, legal, or compliance issues.

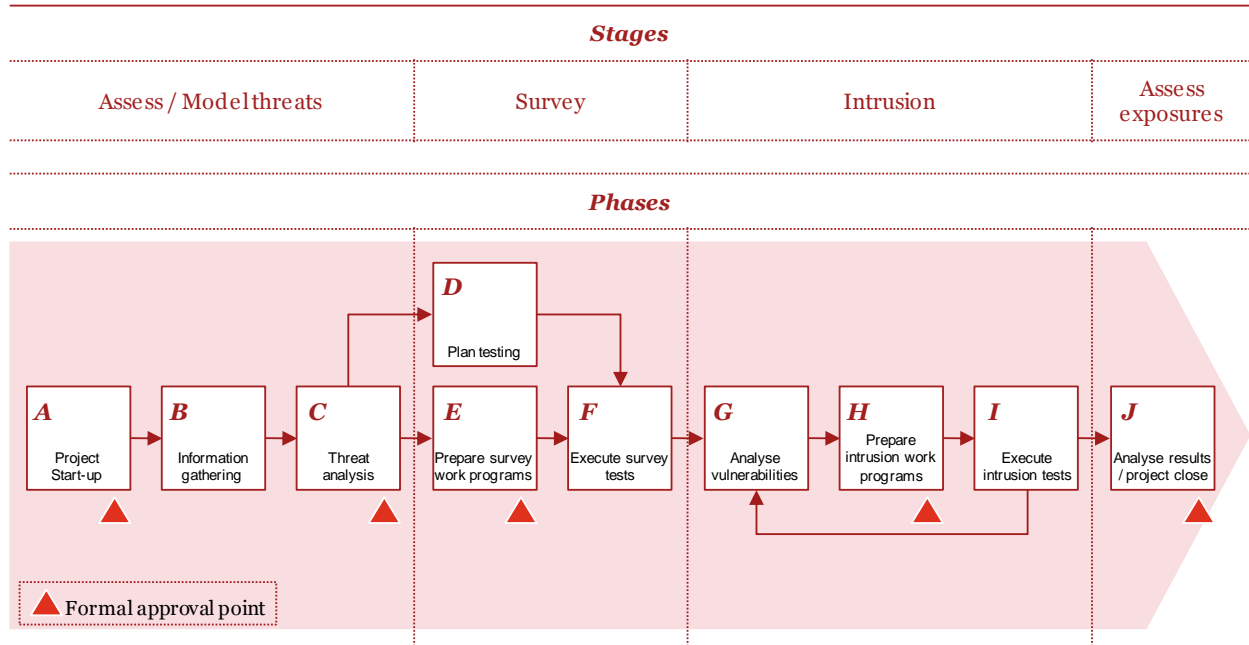
Limitations of testing

We did not perform any active testing for Denial of Service (DoS) vulnerabilities on systems or applications, although where it is suspected that systems are vulnerable to DoS attacks, these have been brought to your attention in this report.

Exploitation of identified vulnerabilities was excluded from the scope, as detailed in our TAL. Therefore, we may have reported vulnerabilities that are not exploitable either due to a false positive or other mitigating controls. Furthermore, there may exist other vulnerabilities beyond those reported here that can only be uncovered through exploitation of one of the identified findings.

Testing methodology

All testing performed during this engagement was conducted in line with PwC's proprietary methodology designed to manage the associated risks inherent with this type of activity. Our methodology is aligned with the CESG CHECK Scheme standards and other widely recognised methodologies such that provided by OWASP.



7. Appendix C: Risk Ratings

All findings in this report have been assigned a risk rating by our team. The risk rating is calculated taking into account the following factors:

- likelihood of vulnerability being exploited;
- ease of exploitation;
- resulting level of access to the host and the network; and
- business impact.

The ratings are based on our understanding of the technical vulnerability, the threat landscape and the business context of the system or application in question. However, they are intended as a guide and you should review each rating in line with your own knowledge of the technical environment and business context.

Definition of Risk

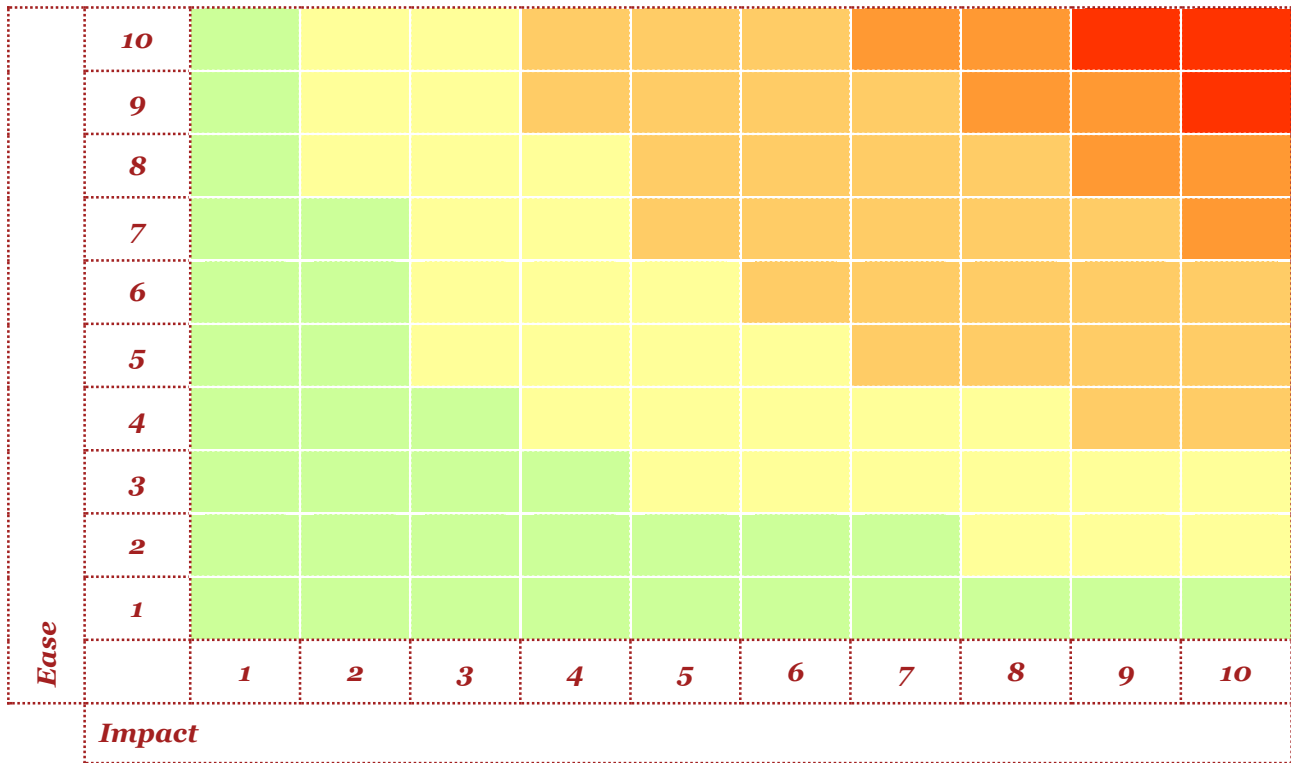
A guide to the ratings and examples of vulnerabilities that fall into each rating can be found below.

Score	Description
Critical	The threat agent would gain full control over the system or application; that is <i>administrative, root or enable</i> access. This would also relate to attacks that would render the system or its data unusable, or irreparably damage the company's reputation. The threat agent can obtain highly sensitive information that if made public could cause considerable damage to the company.
High	The threat agent would gain some kind of interactive control, for example a user account through brute forcing, or control of the system through a low-privilege service. This would also be used in reference to vulnerabilities enabling a threat agent to access information (such as client data) on a host.
Medium	Medium risk vulnerabilities relate to issues that would not lead to a direct compromise of the system or data but could be used to gain further access. This could include local exploits to increase privilege (e.g. a user becoming an administrator), poor security on data (e.g. lack of encryption on key files or network communications). These would often be used in a chained attack.
Low	This would relate to issues such as information leakage, for example a threat agent being able to gather usernames, internal addressing information or other potentially sensitive data.
Info	These issues appear to present only marginal levels of risk but are included as it is felt that they could be used to gain more information about the organisation or systems that may increase the risk to other systems.

When calculating risk ratings we have reproduced steps similar to those included in widely used risk management frameworks. However, due to the technical nature of our work, certain factors used in such frameworks are not included, such as asset values.

To that end we have calculated the risk rating associated with each finding as a product of two key factors; Impact and Ease. These factors have been rated on a numerical scale from one to ten. Details of the definitions of these factors are included in the following section.

Risk ratings are then calculated according to the following heat map.



Definition of Impact

Impact is an indication of the potential implications that could arise from successful exploitation of the vulnerability. This may include financial costs, loss of business, reputational damage, fines or regulatory interest. It could also include technical impact such as establishing a foothold on a network or an ability to access other systems or data.

For example, if an external threat agent could remotely compromise a system hosting financial information this would be defined as a high impact. Similarly, if a vulnerability provided an external threat agent with technical information about the system but did not directly allow them to accomplish anything material this would be a low impact.

Scoring for Impact is defined in the table below.

Score	Description
9 – 10	An attacker could significantly affect the confidentiality, integrity, or availability of the target system through the vulnerability, such as through the ability to remotely administer the system, steal critical business data, or cause a DoS lasting for a long duration. The attacker may also be able to cause a significant amount of reputational damage with successful exploitation of the vulnerability or through the disclosure of sensitive information.

Score	Description
7 – 8	The confidentiality, integrity, or availability of the system would be affected, although to a more limited extent to that above.
5 – 6	The threat agent would be able to disrupt day-to-day operations of the systems, through vulnerabilities such as privilege escalation.
3 – 4	The impact associated with this on systems would be minimal and would not likely be noticed. Examples would include a small degradation in system performance.
1 – 2	It is likely that the impact of a successful exploitation of the vulnerability would not be noticed by the organisation and the threat agent would not be able to assert any level of control over systems.

Definition of Ease

Ease quantifies how complex a given vulnerability is to exploit by an attacker. This includes the skill level required to exploit the vulnerability, whether special circumstances are required in order to carry out the exploit, such as local network access, and whether tools are publically available to automate the exploit.

For example, if the vulnerability required no specialist knowledge, skills, or equipment then it would be very easy to exploit. Similarly, if the vulnerability would require significant technical expertise and knowledge to exploit it would be rated as more complex.

Scoring for Ease is defined in the table below.

Score	Description
9 – 10	The threat agent would require little to no technical knowledge or motivation in order to compromise systems, as the vulnerability could be exploited easily using publicly available information and tools. No special circumstances are required in order to exploit the vulnerability.
7 – 8	A basic technical knowledge or motivation would allow the threat agent to successfully exploit vulnerabilities.
5 – 6	The threat agent would require moderate levels of technical knowledge or motivation in order to exploit the vulnerabilities, for example an understanding and appreciation of programming. Alternatively, the attacker would need to be in a privileged position, such as in a position to intercept network traffic.
3 – 4	Good levels of technical knowledge or motivation in order to exploit the vulnerabilities, for example a working knowledge of programming to modify existing exploits.
1 – 2	The threat agent would require advanced levels of technical knowledge or motivation in order to exploit the vulnerability, for example the ability to research new exploits and create bespoke code.

Limitations of risk ratings

The assessed level of Impact, Ease, and associated Risk scoring presented here is subjective. The scoring process is also limited as a result of not having a true and complete picture of the systems and solutions, or the full knowledge of the value of these systems and solutions. It may be the case that the true level of risk associated with a given vulnerability is higher, or indeed lower, than that stated here, as the value of the assets and systems to the organization has not been incorporated directly into this risk assessment.

8. Appendix D: Affected Hosts

EXT-02. Missing Patches

This table details hosts with identified Missing Patches

**Note that printers are excluded from this list.*

	Microsoft Sharepoint	OpenSSL	Apache
136.148.38.102		✓	
136.148.38.136	✓		
136.148.38.155			✓
136.148.38.156			✓
136.148.38.157		✓	
136.148.38.164			✓

EXT-03. Encryption Weaknesses

This table details hosts with identified Encryption Weaknesses

**Note that printers are excluded from this list.*

	Certificates	SSL v2 and v3	POODLE	Weak Ciphers
136.148.35.142	✓	✓	✓	
136.148.35.150	✓	✓	✓	
136.148.38.121	✓	✓	✓	✓
136.148.38.155	✓	✓	✓	
136.148.233.249	✓	✓	✓	✓

EXT-04. Frameable Responses

The following hosts are vulnerable to clickjacking;

136.148.38.155

136.148.38.106

136.148.38.164

136.148.38.156

136.148.38.92

136.148.61.49

136.148.38.102

136.148.38.121

EXT-05. Information Disclosure

This table details hosts disclosed unnecessary information

**Note that printers are excluded from this list.*

	Default Files	Web Directories	Server Headers	Error Messages
136.148.35.142	✓		✓	
136.148.38.80			✓	
136.148.38.92			✓	
136.148.38.102	✓		✓	
136.148.38.106			✓	
136.148.38.121			✓	
136.148.38.126			✓	
136.148.38.136			✓	
136.148.38.150			✓	
136.148.38.155		✓	✓	✓
136.148.38.156	✓	✓	✓	
136.148.38.157			✓	
136.148.38.164		✓	✓	
136.148.38.177			✓	
136.148.38.236			✓	
136.148.61.45			✓	
136.148.61.49			✓	

EXT-06. Closed ports

This table details hosts disclosed unnecessary information

**Note that printers are excluded from this list.*

	TCP Port 22	TCP Port 993	TCP Port 143	TCP Port 8443	TCP Port 443	TCP Port 8080	TCP Port 8000
136.148.38.92	✓						
136.148.38.102	✓						
136.148.38.106	✓				✓		
136.148.38.121	✓						
136.148.38.126	✓						
136.148.38.132					✓	✓	
136.148.38.136	✓						
136.148.38.156	✓						
136.148.38.157	✓						
136.148.38.236					✓		
136.148.61.45		✓	✓				
136.148.61.49		✓	✓	✓			✓
136.148.77.111		✓	✓				

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.

© 2016 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.

	CONFIDENTIAL
Paper title:	Continuous Audit Report into Prevent Duties
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Ian Mehrtens – Chief Operating Officer
Purpose:	To provide Committee with the results of the review into University obligations relating to the Government’s Prevent Strategy.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This report relates to safeguarding activity across all academic areas, and risk related to the reputation and compliance risk types expressed within the Risk Appetite.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

The 2015 Counter Terrorism and Security Act provided a statutory basis for the obligations which had previously been introduced to institutions regarding the safeguarding of students and stakeholders engaged with activities delivered by the University.

This report reviewed the strategy and approach taken at LSBU against this duty, and is classified as low risk, and has 2 medium, and 2 advisory findings.

These are detailed on pages 6 – 9, and include an action around updating the ICT policy and a revised approach to restricted content, & the creation of a centralised event listing. Good practice recognised by the review is featured in appendix D on page 19.

- The Committee is requested to note the report and its findings.

Internal Audit Report 2015/2016

Prevent Duties

*London South Bank
University*

*Final
August 2016*

▶ Click to launch


Page 80

Contents

Executive Summary

1 

Background and Scope

2 

Findings

Page 81 **3** 

Appendices

- A. Basis of our classifications
- B. Terms of reference
- C. Limitations and responsibilities
- D. Best practice and insight

Distribution list

For action: Ian Mehrtens - Chief Operating Officer
Ed Spacey - Head of Health, Safety and Resilience

For information: Richard Flatman - Chief Financial Officer
John Baker - Corporate and Business Planning Manager
Audit Committee



Executive summary

Report classification

Low Risk



Trend

N/a

We have not performed a review in this area before

Total number of findings

	Critical	High	Medium	Low	Advisory
Control design	0	0	2	0	2
Operating effectiveness	0	0	0	0	0
Total	0	0	2	0	2



Summary of findings

UK Higher Education Institutions (HEIs) have a statutory duty to uphold freedom of speech in their institutions as far as is practical within the law. This duty has come under pressure recently from the Government's Prevent Strategy and provisions in the Counter-Terrorism and Security Act 2015. London South Bank University (LSBU) has created a Safeguarding Strategy which outlines their approach to wider student safeguarding and should address their Prevent responsibilities. The purpose of this audit was to review the strategy and validate the processes and controls in place. We identified two *medium risk* findings:

- HEFCE requires that HEIs outline their Prevent duties within their ICT policies. LSBU's ICT policy does not currently reference Prevent. We also noted that there are currently no filters on mobile devices - including phones, tablets and expert systems (media labs for example) - to block access to extremist materials or Prevent-specific filters within LSBU's network which could allow access to extremist websites. LSBU's Information Security team run a weekly report to identify the 25 "worst offenders" attempting to access blocked websites. This control could be strengthened by including Prevent-specific reporting. **See finding #1.**
- LSBU do not retain a centralised listing of external speakers and events affiliated with them. Lack of central oversight could lead to students being exposed to inappropriate speakers or events. **See finding #2.**

We also identified two *advisory* findings relating to plans for increasing student engagement and Prevent training for employees. **See finding #3 and finding #4.**

Background and scope (1 of 2)



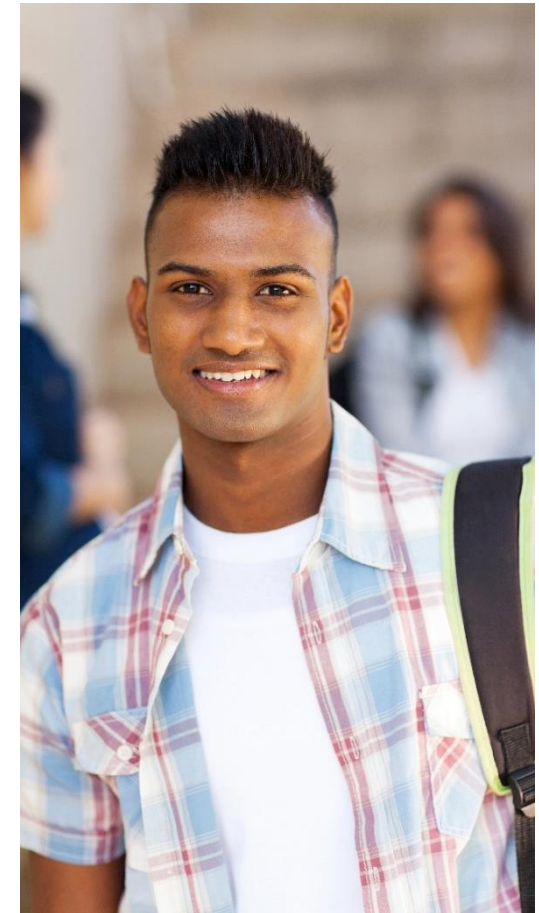
Background

HEIs have a statutory duty to uphold freedom of speech in their institutions as far as is practical within the law. This duty has come under pressure recently from the Government's Prevent Strategy and provisions in the Counter-Terrorism and Security Act 2015.

In the last few years there have been a number of ex-students from UK Universities who have been involved in terrorist activity and it has been suggested that those individuals were radicalised during their studies. Despite a number of steps undertaken by Universities to combat the issue the Government suggested that more could be done in this area and as a result introduced the Prevent Strategy (Prevent). Measures in the Prevent Strategy were out onto statutory basis in the Counter Terrorism and Security Act 2015.

Prevent Duty Guidance for England and Wales has been issued which outlines the expectations for the higher education sector. All higher education institutions to which the duty applies are now defined as Relevant Higher Education Bodies (RHEBs). There is still further guidance to be issued, in particular in relation to the management of external speakers and events.

LSBU has created a Safeguarding Strategy which outlines their approach to wider student safeguarding and should address their Prevent responsibilities. The purpose of this audit was to review the strategy and validate the processes and controls in place.



Background and scope (2 of 2)



Scope

We have reviewed the Safeguarding Strategy and confirm whether it satisfies the requirements of the new Prevent duty. This covered the following areas:

1. Arrangements for senior management and governance oversight of the implementation of the institution's 'Prevent' duty obligations and engagement with 'Prevent' partners.
2. 'Prevent' risk assessment.
3. Action plan in response to that risk assessment.
4. Arrangements for engaging with and consulting students on the institution's plans for implementing the 'Prevent' duty.
5. Staff training plan.
6. Arrangements for sharing information internally and externally about vulnerable individuals.
7. Code of practice for ensuring freedom of speech on campus.

8. Arrangements to protect the importance of academic freedom.

9. Policies and procedures for approving external speakers and events on campus.

10. Policies and procedures for approving RHEB-branded events taking place off campus.

11. Arrangements for sharing information about external speakers with other institutions.

12. Arrangements to ensure sufficient pastoral care and chaplaincy support for all students (including arrangements for managing prayer and faith facilities).

13. Policies for use of the institution's computer facilities (hardware, software, networks, social media), to including consideration of filtering arrangements and management of academic activities that might require access to sensitive or terrorism-related material.

14. Arrangements for engaging with students' unions and societies (which are not subject to the 'Prevent' duty, but are expected to cooperate with their institution).

Limitations of scope

Our review was limited to the elements of the process outlined above. The scope of the review was limited to the Counter Terrorism and Security Act legislation only.

IT Policies
Control design

1

Page 55 of 55

Finding rating

Rating

Medium

Findings

HEFCE requires that HEIs outline their Prevent duties within their ICT policies. LSBU's ICT policy does not currently reference Prevent. We also noted that:

- There are no filters on mobile devices - including phones, tablets and expert systems (e.g. media labs) - to block access to extremist materials.
- There are no Prevent-specific filters within LSBU's network. We note that alternative filters are available covering violence, weapons etc.
- The Information Security team run a weekly report to identify the 25 "worst offenders" attempting to access blocked websites. This control could be strengthened by including Prevent-specific reporting.

Implications

Insufficient information security controls could allow individuals to access inappropriate web content. This could mean that LSBU is not complying fulfilling their Prevent duties which could result in reputational or financial damage.

Action plan

- We will update the ICT policy to include Prevent.
- We will look into options to implement Prevent-specific filters within LSBU's network and also applying filters to mobile devices.
- We will produce a weekly report on attempts to access restricted content. This will be shared with the Chief Operating Officer as required.

Responsible person/title:

Craig Girvan (Head of Information Security)

Target date:

30/09/2016

Reference number:

1

External Speakers and Events

Control design

2

Page 86 of 97

Finding rating

Rating

Medium

Finding

The Prevent Duty guidance states that LSBU should have policies and procedures in place for approving external speakers and events, on and off campus. A complete listing of LSBU affiliated events is not currently retained. This is due to events being managed by a number of different teams.

Implications

Without a complete listing of events, there may be insufficient oversight of speakers or events taking place in connection with LSBU. This could result in vulnerable individuals coming into contact with extremist content or speakers.

Action plan

- We will prepare a centralised listing of LSBU affiliated events taking place both on and off campus.

Responsible person/title:

Ed Spacey (Head of Health Safety and Resilience)

Target date:

31/12/2016

Reference number:

2

Student Engagement

Control design

3

Finding

A Student Engagement Plan had not been formalised at the time of audit fieldwork.

Implications

If LSBU does not have a Student Engagement Plan outlining how they plan to effectively communicate the requirements and impact of Prevent, LSBU's students may be unaware or disengaged with the Prevent initiative.

Action plan

- We will formalise our Student Engagement Plan.

Responsible person/title:

Ed Spacey (Head of Health Safety and Resilience)

Target date:

31/12/2016

Reference number:

3

Page 27 of 77

Finding rating

Rating

Advisory

Staff Training Plan

Control design

4

Page 88 of 97

Finding rating

Rating

Advisory

Finding

LSBU plans to deliver staff training in four tiers. Tier 1 training has been finalised and all employees are required to complete the training by 30 September 2016.

Training material for tiers 2, 3 and 4 is still being developed and LSBU has not agreed a timetable for when training will be delivered.

Implications

A delay in delivering the tier 2, 3 and 4 training could result in staff not understanding their roles and responsibilities relating to Prevent.

Action plan

- We will finalise training materials for tier 2, 3 and 4 training and implement a timetable to deliver this training.

Responsible person/title:

Ed Spacey (Head of Health Safety and Resilience)

Target date:

31/12/2016

Reference number:

4



**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

**Appendix D: Best practice
and insight**

Appendices

Appendix A: Basis of our classifications

Individual finding ratings

Critical

A finding that could have a:

- **Critical** impact on operational performance resulting in inability to continue core activities for more than two days; or
- **Critical** monetary or financial statement impact £5m; or
- **Critical** breach in laws and regulations that could result in material fines or consequences over £500k; or
- **Critical** 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.

High

A finding that could have a:

- **Significant** impact on operational performance resulting in significant disruption to core activities; or
- **Significant** monetary or financial statement impact of £2m; or
- **Significant** breach in laws and regulations resulting in significant fines and consequences over £250k; or
- **Significant** impact on the reputation or brand of the organisation, resulting in unfavourable national media coverage.

Medium

A finding that could have a:

- **Moderate** impact on operational performance resulting in moderate disruption of core activities or significant disruption of discrete non-core activities; or
- **Moderate** monetary or financial statement impact of £1m; or
- **Moderate** breach in laws and regulations resulting in fines and consequences over £100k; or
- **Moderate** impact on the reputation or brand of the organisation, resulting in limited unfavourable media coverage.

Appendix A: Basis of our classifications

Individual finding ratings

Low

A finding that could have a:

- **Minor** impact on the organisation’s operational performance resulting in moderate disruption of discrete non-core activities; or
- **Minor** monetary or financial statement impact of £500k; or
- **Minor** breach in laws and regulations with limited consequences over £50k; or
- **Minor** impact on the reputation of the organisation, resulting in limited unfavourable media coverage restricted to the local press.

Advisory

A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Report classifications

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

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

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

Appendix B: Terms of reference

London South Bank University

Terms of reference – Prevent Duties

To: **Ian Mehrtens (Chief Operating Officer)**

From: **Justin Martin (Head of Internal Audit)**

This review is being undertaken as part of the 2015/16 internal audit plan approved by the Audit Committee.

Background

UK Higher Education Institutions (HEIs) have a statutory duty to uphold freedom of speech in their institutions as far as is practical within the law. This duty has come under pressure recently from the Government's Prevent Strategy and provisions in the Counter-Terrorism and Security Act 2015.

In the last few years there have been a number of ex-students from UK Universities who have been involved in terrorist activity and it has been suggested that those individuals were radicalised during their studies. Despite a number of steps undertaken by Universities to combat the issue the Government suggested that more could be done in this area and as a result introduced the Prevent Strategy (Prevent). Measures in the Prevent Strategy were out onto statutory basis in the Counter Terrorism and Security Act 2015.

Prevent Duty Guidance for England and Wales has been issued which outlines the expectations for the higher education sector. All higher education institutions to which the duty applies are now defined as Relevant Higher Education Bodies (RHEBs). There is still further guidance to be issued, in particular in relation to the management of external speakers and events.

London South Bank University (LSBU) have created a Safeguarding Strategy which outlines their approach to wider student safeguarding and should address their Prevent responsibilities. The purpose of this audit is to review the strategy and validate the processes and controls in place.

Appendix B: Terms of reference

We believe our work will touch upon the following areas of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management
10				x	x

x = area of primary focus x = possible area of secondary focus

Scope

We will review the Safeguarding Strategy and confirm whether it satisfies the requirements of the new Prevent duty:

1. Arrangements for senior management and governance oversight of the implementation of the institution's 'Prevent' duty obligations and engagement with 'Prevent' partners.
2. 'Prevent' risk assessment.
3. Action plan in response to that risk assessment.
4. Arrangements for engaging with and consulting students on the institution's plans for implementing the 'Prevent' duty.
5. Staff training plan.
6. Arrangements for sharing information internally and externally about vulnerable individuals.
7. Code of practice for ensuring freedom of speech on campus.
8. Arrangements to protect the importance of academic freedom.

Appendix B: Terms of reference

9. Policies and procedures for approving external speakers and events on campus.
10. Policies and procedures for approving RHEB-branded events taking place off campus.
11. Arrangements for sharing information about external speakers with other institutions.
12. Arrangements to ensure sufficient pastoral care and chaplaincy support for all students (including arrangements for managing prayer and faith facilities).
13. Policies for use of the institution's computer facilities (hardware, software, networks, social media), to including consideration of filtering arrangements and management of academic activities that might require access to sensitive or terrorism-related material.
14. Arrangements for engaging with students' unions and societies (which are not subject to the 'Prevent' duty, but are expected to cooperate with their institution).
As part of this we will assess the design of controls and their operating effectiveness.

Limitations of scope

Our review will be limited to the elements of the process outlined above. The scope of the review is limited to the Counter Terrorism and Security Act legislation only.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the process through discussions with key personnel, review of methodology and procedure notes and walkthrough tests;
- Identify the key risks relating to the process;
- Evaluate the design of the controls in place to address the key risks;
- Test the operating effectiveness of the key controls.

Appendix B: Terms of reference

Internal audit team

Name	Title	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@uk.pwc.com
Charlotte Bilsland	Engagement Senior Manager	07718 484 470 charlotte.bilsland@uk.pwc.com
Lucy Gresswell	Engagement Supervisor	07718 098 321 lucy.j.gresswell@uk.pwc.com

Key contacts

Name	Title	Contact details	Responsibilities
Ian Mehrtens	Chief Operating Officer (Audit Sponsor)	020 7815 6804 ian.mehrtens@lsbu.ac.uk	Review and approve terms of reference Review draft report Review and approve final report
Ed Spacey	Head of Health, Safety and Resilience (Audit Contact)	0207 815 6831 spaceye@lsbu.ac.uk	Hold initial scoping meeting Review and meet to discuss issues arising and develop management responses and action plan
Richard Flatman	Chief Financial Officer (Audit Contact)	0207 815 6301 richard.flatman@lsbu.ac.uk	Receive draft and final terms of reference Receive draft report
John Baker	Corporate and Business Planning Manager (Audit Contact)	0207 815 6003 j.baker@lsbu.ac.uk	Receive final report

Appendix B: Terms of reference

Timetable

Fieldwork start	23/05/2016
Fieldwork completed	03/06/2016
Draft report to client	10/06/2016
Response from client	24/06/2016
Final report to client	01/07/2016

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;
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. 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.

Future periods

Our assessment of controls is for the period specified only. 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 changes; or
- The degree of compliance with policies and procedures may deteriorate.

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 endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we 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.

Appendix D: Good practice and insight

Areas of Good Practice

LSBU has applied a proactive approach to the Prevent Duty guidance. LSBU has worked closely with HEFCE to ensure that it is complying with the guidance and has received positive feedback from HEFCE regarding the progress made.

Page 98

Insight: Prevent – what does it mean for higher education?

The PwC Public Sector Research Centre (PSRC) produced a thought leadership piece in Spring 2016 outlining some questions for Universities to consider when preparing their response to Prevent. This article, and other thought leadership from the PSRC, can be viewed within the following link:

<http://www.pwc.co.uk/industries/government-public-sector/education/he-matters/people-special-2016/prevent-what-does-it-mean-for-higher-education.html>



This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to the Memorandum of Assurance and Accountability (MMA) between Higher Education Funding Council for England (HEFCE) and institutions. 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.

In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), London South Bank University is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, London South Bank University discloses any this document 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.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Continuous Audit Report into Risk Management
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with the results of the annual Internal Audit review into the University’s strategy and approach to enterprise risk management.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This report relates to the management of risk related to all of the goals of the Corporate Strategy.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

The attached report provides the results of this review of Risk Management – undertaken as part of the annual internal audit programme in 15/16.

The report classification is low risk, with one medium, and two advisory recommendations. (*pages 6 – 9*)

The medium finding relates to the completeness of records in some operational areas.

- The Committee is requested to note the report and its findings.

Internal Audit Report 2015/2016

Risk Management

London South Bank
University

September 2016

Final


Page 102 [Click to launch](#)

Contents

Executive summary

1 

Background and scope

2 

Findings

Page 103 **3** 

Appendices

- A. Basis of our classifications
- B. Terms of reference
- C. Limitations and responsibilities
- D. Managing risk in higher education

Distribution list

For action: John Baker - Corporate and Business Planning Manager

For information: Richard Flatman - Chief Financial Officer
Audit Committee



Executive summary

Report classification

Low Risk



Trend



Performance is consistent with the 2014/15 review.

Total number of findings

	Critical	High	Medium	Low	Advisory
Control design	0	0	0	0	0
Operating effectiveness	0	0	1	0	2
Total	0	0	1	0	2

Page 104



Summary of findings

We identified one *medium* risk finding:

- We tested a sample of five Professional Service Department (PSD) and School's operational risk registers to confirm that these were being fully completed and reviewed on a timely basis. We identified a number of instances where the risk registers did not appear to be complete, risks and actions weren't specific and required actions had not been implemented by the agreed completion date. **See finding #2.**

We identified the following *advisory* findings where improvements could be made:

- We reviewed the Corporate Risk Register to confirm that it was complete, up-to-date and appropriately documented. We identified that mitigating controls were missing for two of the 14 risks. **See finding #1.**
- We reviewed the actions points from the annual business review meetings and business plans for a sample of five PSD's and School's. We found instances whereby the defined risks were vague and not 'true risks'. There were also a number of agreed actions without a person responsible assigned or a target completion date. **See finding #3.**

Background and scope (1 of 2)



Background

Effective risk management is essential in helping any organisation to improve governance, focus decision making and achieve objectives. Risk management is ensured through maintenance of risk registers and an awareness of risk throughout within an organisation. HEFCE direction states that institutions are required to have effective risk management policies and processes that cover all significant risks, assess exposure and regularly monitor risk to ensure effective governance.

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.

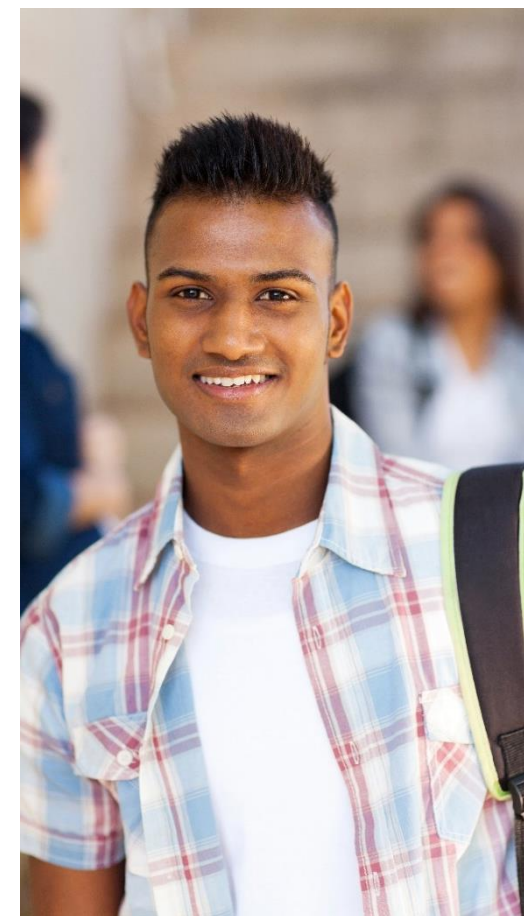
The ability of an organisation to successfully implement effective risk management arrangements in order to take advantage of these benefits is heavily dependent on staff and officers having an understanding of their responsibilities together with the principles and processes that underpin effective 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.

Our work touched upon the following areas of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management
5	x			x	x

x = area of primary focus

x = possible area of secondary focus



Background and scope (2 of 2)



Scope and limitations of scope

Our review included the following sub-processes and key control objectives:

<i>Sub-process</i>	<i>Key control objectives</i>
<i>Risk Strategy</i>	<ul style="list-style-type: none"> Vision, commitment and ownership of risk management are defined within London South Bank University (LSBU). Roles and responsibilities are clearly defined. Risks – at a corporate and operational level - are aligned to the LSBU’s Strategic Plan.
<i>Statement of Risk Appetite</i>	<ul style="list-style-type: none"> The Risk Appetite is defined and is considered in the management of risk and resource allocation. Sufficient data is captured to allow the organisation to assess performance against Risk Appetite.
<i>Risk identification</i>	<ul style="list-style-type: none"> The risk identification process encourages the identification of risk, an assessment of magnitude, likelihood and impact at all levels of LSBU, with key partners and is a continuous process. There is clear ownership and responsibility for managing key risks at an operational level.
<i>Monitoring and reporting</i>	<ul style="list-style-type: none"> Risks are regularly monitored and mitigation measures updated. This is reported to a sufficient level of management to ensure awareness and recognition of risks at a corporate level.

Limitations of scope

Our work was limited to the procedures outlined in the table above.

Our testing on Risk Strategy and Risk Appetite was limited to checking that these documents have been reviewed by the Executive Board on an annual basis.

The majority of our testing was focussed on testing the Corporate Risk Register and a sample of PSD and School risk registers. We did not interview PSDs or School’s as part of this review; our work was limited to a desktop review of operational plans only.

Our work did not include any testing of contract or project risk registers.

Corporate Risk Register

Operating effectiveness

1

Page 107

Finding rating

Rating

Advisory

Findings

We reviewed the Corporate Risk Register to test whether the register was complete, up-to-date and appropriately documented.

We found two of the 14 risks in the Corporate Risk Register do not have an associated risk control. These are:

- 1) Risk Ref: 494 - Inconsistent delivery of Placement activity across institution
- 2) Risk Ref: 495 - Impact of Higher Apprenticeship degrees on existing recruitment markets.

We note from discussion with management that emerging findings do not initially have a control in place until the risk is fully understood.

Implications

The absence of risk controls in the Corporate Risk Register could indicate that risks are not being proactively mitigated. This could expose LSBU to risk.

Action plan

Controls are developed within a timeframe relevant to the nature of the risk. In some instances it may not be possible to implement a suitable control. The Strategic Risk Review Group and Operations Board will consider what controls could be developed in relation to these emerging risks, amending risk register entries as appropriate.

Responsible person/title:

John Baker, Corporate and Business Planning Manager

Target date:

30/11/2016

Reference number:

1

Organisational Risk Registers

Operating effectiveness

Page 108

2

Finding rating

Rating

Medium

Findings

We reviewed the risk register's in place for five PSD's and Schools. We found the following:

Completeness

- On the Finance and Management Information risk register, the cause and effect column is incomplete for two of the 21 risks, the controls column is incomplete for three of the 21 risks. We understand that there may not be a suitable control for LSBU to implement in response to these three risks.
- The cause and effect column is incomplete for one of the 13 risks on the Academic Related Resources risk register.
- The cause and effect column is incomplete for three of the eight risks on the Marketing Recruitment and Admissions risk register.

Timeliness

- The risk registers do not retain an audit trail identifying when the register was last updated.
- For four of the 17 agreed actions outlined in the Finance and Management Information risk register, the implementation date had been passed at the date of audit fieldwork. We note that a progress report was prepared which provided an update on two of these actions.
- For the one agreed action outlined in the Academic Related Resources risk register, the implementation date had been passed at the date of audit fieldwork.
- For nine of the 12 agreed actions outlined in the Built Environment and Architecture risk register, the implementation date had been passed at the date of audit fieldwork.

Agreed Action Identification

- A number of the actions outlined in the risk register were not specific. For example:
 - The risk register for Built Environment and Architecture includes the following as an action required: "Increase the number of visits to local schools, colleges and academies". As this is not specific, it will be difficult for LSBU to identify whether the action has been implemented. An alternative action could be: "LSBU shall visit 20 of local schools, colleges and academies".

Organisational Risk Registers

Operating effectiveness

Continued

2

Page 109

Finding rating

Rating

Medium

Findings (continued)

Risk Identification

- A number of the risks are not 'truly risks'. For example:
 - Built Environment and Architecture
 - Risk 241: Inability to integrate apprenticeships; and
 - Marketing and Engagement
 - Risk 404, Indemnity Insurance

These are risk titles/areas not a risk. Instead, the PSD/School should define its objectives and then consider what scenarios would prevent this from being achieved.

Implications

- Incomplete risk registers could indicate that risks are not being proactively managed. This could expose LSBU to risk.
- If risks are not monitored on a timely basis, the risk profile may be incorrect meaning LSBU cannot appropriately assess threats or vulnerabilities.
- If risks are not clearly defined and aligned to objectives then inadequate controls may be implemented. This could mean the risk profile is over or under stated and managed inappropriately. Alignment of individual risks to objectives, will allow the organisation to prioritise and focus on critical risks.

Action plan

- The new 4-risk system records historical changes to risk entries, however the system is currently not set-up to export changes in each PSD/ School. We will introduce reporting on changes made at the PSD/ School level.
- We will review the organisational risk registers and send reminders to risk owners to complete all mandatory fields.

Responsible person/title:

John Baker, Corporate & Business Planning Manager

Target date:

31/07/2017

Reference number:

2

Risk review

Operating effectiveness

Page 110

3

Finding rating

Rating

Advisory

Findings

Business review meetings were previously held on a quarterly basis for each School and PSD. This is now an annual process. Minutes are no longer produced from these meetings, we were only able to review action points. We reviewed action points prepared for five Schools and PSDs, we found:

- 1) For Finance and Management Information, none of the ten action points listed had a target completion date.
- 2) For Academic Related Resources, none of the ten action points listed had a target completion date. Five of the ten actions had either 'TBC' or 'Director' listed as the person responsible for implementing the action.
- 3) For Marketing Recruitment and Admissions, none of the six actions had a target completion date.
- 4) For Built Environment and Architecture, none of the ten action points listed had a target completion date or person assigned to implement the action.

Each School and PSD is required to document their top three challenges (or risks) in their annual business plan. We reviewed the Business Plans for the same five Schools and PSDs, we found:

- 1) For Finance and Management - the three top challenges do not read as true challenges or risks to the achievement of the PSD's objectives. For example: "Embedding a revised investment appraisal process, and contributing to effective benefit tracking and impact reporting".
- 2) For Academic Related Resources - the three challenges are not identified.

Implications

If challenges or risks to the School and PSD are not identified in the annual business plan, LSBU may be unable to put appropriate controls in place to mitigate the risk.

If actions do not have a target completion date or appropriate person responsible for it's implementation, this could mean that actions are not implemented in a timely manner, meaning LSBU is vulnerable to risk.

Risk review

Operating effectiveness

Continued

3

Page 11

Finding rating

Rating

Advisory

Action plan

- We will perform a review of the annual action points and business plan for all PSDs and Schools to ensure all fields are complete and appropriate.

Responsible person/title:

John Baker, Corporate & Business Planning Manager

Target date:

30/11/2016

Reference number:

3



**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

**Appendix D: Managing risk
in higher education**

Appendices

Appendix A: Basis of our classifications

Individual finding ratings

Critical

A finding that could have a:

- **Critical** impact on operational performance resulting in inability to continue core activities for more than two days; or
- **Critical** monetary or financial statement impact £5m; or
- **Critical** breach in laws and regulations that could result in material fines or consequences over £500k; or
- **Critical** 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.

High

A finding that could have a:

- **Significant** impact on operational performance resulting in significant disruption to core activities; or
- **Significant** monetary or financial statement impact of £2m; or
- **Significant** breach in laws and regulations resulting in significant fines and consequences over £250k; or
- **Significant** impact on the reputation or brand of the organisation, resulting in unfavourable national media coverage.

Medium

A finding that could have a:

- **Moderate** impact on operational performance resulting in moderate disruption of core activities or significant disruption of discrete non-core activities; or
- **Moderate** monetary or financial statement impact of £1m; or
- **Moderate** breach in laws and regulations resulting in fines and consequences over £100k; or
- **Moderate** impact on the reputation or brand of the organisation, resulting in limited unfavourable media coverage.

Appendix A: Basis of our classifications

Individual finding ratings

Low

A finding that could have a:

- **Minor** impact on the organisation’s operational performance resulting in moderate disruption of discrete non-core activities; or
- **Minor** monetary or financial statement impact of £500k; or
- **Minor** breach in laws and regulations with limited consequences over £50k; or
- **Minor** impact on the reputation of the organisation, resulting in limited unfavourable media coverage restricted to the local press.

Advisory

A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Page 114

Report classifications

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

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

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

Appendix B: Terms of reference – Risk Management

To: John Baker - Corporate and Business Planning Manager

From: Justin Martin – Head of Internal Audit

Page 115

Background and audit objectives



This review is being undertaken as part of the 2015/2016 internal audit plan approved by the Audit Committee.

Background and audit objectives

Effective risk management is essential in helping any organisation to improve governance, focus decision making and achieve objectives. Risk management is ensured through maintenance of risk registers and an awareness of risk throughout within an organisation. HEFCE direction states that institutions are required to have effective risk management policies and processes that cover all significant risks, assess exposure and regularly monitor risk to ensure effective governance.

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.

We believe our work will touch upon the following areas of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management	
5	x			x	x	x = area of primary focus x = possible area of secondary focus

Audit scope and approach (1 of 2)



Scope

We will test the following sub-processes.

<i>Sub-process</i>	<i>Key control objectives</i>
<i>Risk Strategy</i>	<ul style="list-style-type: none"> Vision, commitment and ownership of risk management are defined within London South Bank University (LSBU). Roles and responsibilities are clearly defined. Risks – at a corporate and operational level - are aligned to the LSBU’s Strategic Plan.
<i>Statement of Risk Appetite</i>	<ul style="list-style-type: none"> The Risk Appetite is defined and is considered in the management of risk and resource allocation. Sufficient data is captured to allow the organisation to assess performance against Risk Appetite.
<i>Risk identification</i>	<ul style="list-style-type: none"> The risk identification process encourages the identification of risk, an assessment of magnitude, likelihood and impact at all levels of LSBU, with key partners and is a continuous process. There is clear ownership and responsibility for managing key risks at an operational level.
<i>Monitoring and reporting</i>	<ul style="list-style-type: none"> Risks are regularly monitored and mitigation measures updated. This is reported to a sufficient level of management to ensure awareness and recognition of risks at a corporate level.

Audit scope and approach (2 of 2)



Limitations of scope

Our work will be limited to the procedures outlined in the table above.

Our testing on Risk Strategy and Risk Appetite shall be limited to checking that these documents have been reviewed by the Executive Board on an annual basis.

The majority of our testing shall be focussed on testing the Corporate Risk Register and a sample of PSD and School risk registers. We will not be interviewing PSDs or School's as part of this review; our work is limited to a desktop review of operational plans only. We will select a sample of these to test in advance (please see this sample in Appendix 1).

Our work did not include any testing of contract or project risk registers.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the process through discussions with key personnel, review of methodology and procedure notes and walkthrough tests;
- Identify the key risks relating to the process;
- Evaluate the design of the controls in place to address the key risks;
- Test the operating effectiveness of the key controls.

Internal audit team and key contacts



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@uk.pwc.com
Charlotte Bilsland	Engagement Senior Manager	07715 484 470 charlotte.bilsland@uk.pwc.com
Lucy Gresswell	Engagement Supervisor	07718 098 321 lucy.j.gresswell@uk.pwc.com

Key contacts – London South Bank University

Name	Title	Contact details	Responsibilities
Richard Flatman	Chief Financial Officer (Audit Sponsor)	0207 815 6301 richard.flatman@lsbu.ac.uk	Review and approve terms of reference Review draft report Review and approve final report Hold initial scoping meeting Review and meet to discuss issues arising and develop management responses and action plan
John Baker	Corporate and Business Planning Manager (Audit Contact)	0207 815 6003 j.baker@lsbu.ac.uk	Receive draft and final terms of reference Receive draft report Receive final report

Timetable



Timetable

Fieldwork start	11 July 2016
Fieldwork completed	29 July 2016
Draft report to client	12 August 2016
Response from client	26 August 2016
Final report to client	02 September 2016

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.
- Staff and management will make reasonable time available for interviews and will respond promptly to follow-up questions or requests for documentation.

Please note that if the University requests the audit timing to be changed at short notice (2 weeks before fieldwork start) and the audit staff cannot be deployed to other client work, the University may still be charged for all/some of this time. PwC will make every effort to redeploy audit staff in such circumstances.

Information request



Please find attached a deliverables listing outlining items we expect to have available in advance of the audit:

- A copy of the Corporate Risk Register;
- Copies of the Risk Register for the following Schools/ Departments:
 - Governance
 - Procurement
 - Business Engagement and Development
 - The Confucius Institute
 - Built Environment and Architecture
- A copy of the Risk Management Strategy, Risk Appetite and Risk Management Policy;
- Access to any minutes for relevant oversight Boards;
- Evidence of how risks are currently managed.

This listing is not exhaustive, additional items may be asked for on request.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. 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.

Future periods

Our assessment of controls is for the period specified only. 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 changes; or
- The degree of compliance with policies and procedures may deteriorate.

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 endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we 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.

Appendix D: PwC publications: Managing risk in higher education

Insight:

The PwC Public Sector Research Centre (PSRC) produced a recent series of blogs “Managing risk in higher education”. These blogs capture the following topics:

- Bulding Digital Trust: Information systems and technology challenges for the higher education sector
 - The global university: What are the risks of international working?
 - Higher education sector risk profile: What are the key risks faced by HEIs?
- Did you know? Risk trends in higher education

These blogs, and other publications prepared by the PSRC, can be found in the following link:

<http://www.pwc.co.uk/industries/government-public-sector/education/risk-assurance-for-higher-education.html>

Managing Risk in Higher Education: Higher Education Sector Risk Profile - 2016

Alongside this report, we present our 2016 Higher Education risk profiling paper. This paper presents the findings of our benchmarking study of 44 institutions (2015: 40) in terms of what their significant risks were and how those risks were being managed. It also highlights developments and trends in risk management practice across the sector and what we can learn from developments in the commercial sector and beyond.



This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to the Memorandum of Assurance and Accountability (MMA) between Higher Education Funding Council for England (HEFCE) and institutions. 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.

In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), London South Bank University is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, London South Bank University discloses any this document 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.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

	CONFIDENTIAL
Paper title:	Continuous Audit Report into Key Financial Systems
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with the results of the Internal Audit continuous audit review into the University's Key Financial Systems.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This report relates to the Resources and Infrastructure goal of the Corporate Strategy.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

The report relates to the testing which took place in August 2016, reviewing transactions and activity for the period January – July 2016.

Accounts Payable & Receivable, and Cash are all still rated as green, with some minor exceptions. The report found a slight deterioration in the General Ledger, and continuing issues with the Payroll, which are rated as amber.

The audit team found evidence of untimely preparation and authorisation of reconciliations, and starter and leaver documentation was missing, or not authorised on a timely basis.

Control design findings to address these issues are detailed on pages 11, 15, 25 and 26.

- The Committee is requested to note the report and its findings.

Internal Audit Report 2016/2017

Continuous Auditing: Key Financial Systems 2016/17

London South Bank
University

Final
September 2016


Page 126 [Click to launch](#)

Contents

Executive summary

1 

Background and scope

2 

Findings

Page 127 **3** 

Appendices

- A. Basis of our classifications
- B. Terms of reference
- C. Limitations and responsibilities

Distribution list

For action: Natalie Ferer - Financial Controller

For information: Richard Flatman – Chief Financial Officer
John Baker - Corporate & Business Planning Manager
Audit Committee




























Executive summary



System Summaries

There has been a decline in performance this period. Untimely preparation and authorisation of reconciliations is a recurring theme, affecting Payroll and General Ledger. We have also continued to see exceptions affecting starter and leaver documentation within Payroll, which was either missing or has not been authorised on a timely basis.

Our ratings are based on the number and severity of findings noted for controls tested as part of the programme. Our rating criteria are set out at Appendix 1. This does not consider control design issues – these are individually risk rated.

System / Rating	P1 2016/17	P2 2015/16	P1 2015/16	P3 2014/15	Trend
Payroll	 Amber	 Amber	 Green	 Green	
Accounts Payable	 Green	 Green	 Green	 Green	
Accounts Receivable	 Green	 Green	 Green	 Green	
Cash	 Green	 Green	 Green	 Amber	
General Ledger	 Amber	 Green	 Green	 Green	

Background and scope



Background

The purpose of our Continuous Auditing programme is to test key controls on an on-going basis to assess whether they are operating effectively and to flag areas and/or report transactions that appear to circumvent controls. The systems included within the scope of our work in 2016/17 are:

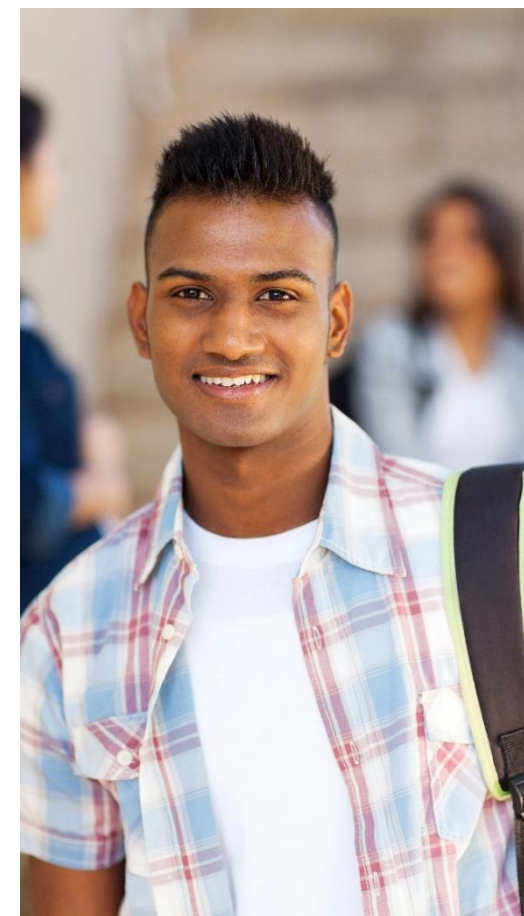
- Payroll;
- Accounts Payable;
- Accounts Receivable;
- Cash; and
- General Ledger.

We have outlined the controls we will be testing in Appendix B. These have been identified through our annual audit planning process and meetings with management to update our understanding of the control framework in place. We will continue to refresh this knowledge throughout the year to ensure we focus upon the key risks facing London South Bank University (LSBU).

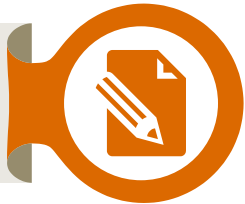
Our detailed findings are set out in Findings section of this report, starting on page 7. A summary of our findings and the matters arising in the course of our work this period is set out below.

Performance Ratings

Performance is indicated either as 'green' or 'red'. 'Green' indicates that there were no operating effectiveness issues noted during the testing period. 'Red' indicates that an exception was identified. Control design issues are raised separately with individual risk ratings.



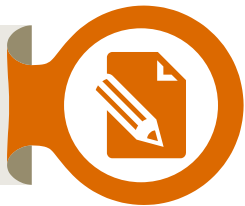
Detailed Findings



Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P1 Authorised and accurate new starter forms are received prior to an individual being entered on to the Payroll system.	●	<ul style="list-style-type: none"> 1/20 new starters sampled did not have a new starter form. For 2/20 new starters, the date on the starter form does not agree to the HR system. <p>Management response:</p> <p>The starter form could be found but was probably misfiled due to changeover of staff and temporary staff not being adequately supervised. This is addressed in control design 1 below.</p> <p>The reason for the discrepancies on start dates are being investigated by the HR team.</p> <p>Responsibility for action:</p> <p>Joanne Monk, Deputy Director of HR/ Denise Sullivan, Head of Payroll and Pensions</p>	●	●	●

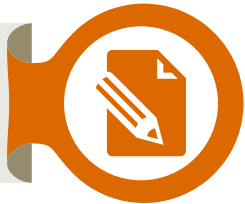
Detailed Findings



Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P2 Leaver forms are received from Human Resources upon notification of resignation or redundancy.	●	<ul style="list-style-type: none"> 2/25 leavers sampled did not have an leaver form. For 4/25 leavers tested, the leaver form was authorised after the employee leave date. The longest delay was 41 days after the individual left LSBU. <p>Management response: The reason for the delay in notifying Payroll of leavers is being investigated by the HR team.</p> <p>Responsibility for action: Joanne Monk, Deputy Director of HR / Denise Sullivan, Head of Payroll and Pensions</p>	●	●	●

Detailed Findings

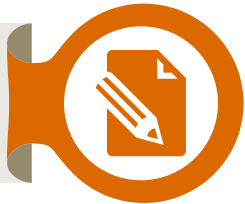


Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P3 The BACS run is reviewed by the Financial Controller and a Payment Release Form completed.	●		●	●	●
P4 Exception reports are produced and reviewed as part of month-end procedures, before the payment run is authorised.*	●		●	●	●

* This included the following reports: Errors and warnings reports (i.e. processing issues encountered); Payroll differences (difference between each element between two periods, with tolerances of between 5% and 10%); Gross pay over £6,000; Number of staff paid in comparison to previous month with subsequent reconciliation; Starters and leavers for the period; Element differences between two periods for overtime and bonuses; and, HMRC payments.

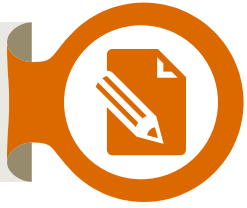
Detailed Findings



Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P5 Variation forms, with supporting documentation, are received prior to any changes being made to standing data.	●		●	●	●
P6 Access to the payroll system is restricted to appropriate personnel.	●		●	●	●

Detailed Findings



Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P7 Appropriately authorised overtime claim forms and timesheets are received prior to payment being made.	●	<ul style="list-style-type: none"> 1/20 overtime claims did not have a supporting overtime form. <p>Management response:</p> <p>The form could be found but was probably misfiled due to changeover of staff and temporary staff not being appropriately supervised. This is addressed in control design 1 below.</p> <p>Responsibility for action:</p> <p>Denise Sullivan, Head of Payroll and Pensions</p>	●	●	●

Detailed Findings



Payroll

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
P8 Monthly reconciliations are performed between the general ledger and the payroll system. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	●	<ul style="list-style-type: none"> 2/20 reconciliations had not been dated when authorised so we could not confirm whether the review was completed in a timely manner. <p>Management response: As with GL4, in the past it has been difficult to monitor that all reconciliations had been completed and authorised in a timely manner. There is now a monthly check list in place which will be used to evidence that all balance sheet accounts have been reviewed monthly and dated to evidence this.</p> <p>Responsibility for action: Rebecca Warren/Sally Black, Financial Accountants</p>	●	●	●
P9 Expenses are supported by appropriately authorised claim forms.	●		●	●	●

Loss of Payroll Documentation
Control Design

1

Page 136

Finding rating

Rating **Medium risk**

Findings

Our payroll testing has identified several instances where management could not provide us with supporting documentation, for example: overtime, variations, starters and leavers. This has been caused by a backlog of filing within the Payroll department.

Implications

- If documentation is not filed appropriately and kept secure then LSBU could find confidential information is accessed by inappropriate personnel. This could have reputational and financial implications under data protection regulations.
- If documentation is not retained, then it is not possible to prove that changes made were/are appropriate.
- Resource may be diverted from important tasks to obtain missing documentation. This could cause delays in processing changes and other key payroll activities.

Action plan

- Going forward one member of staff will be responsible for filing which includes ensuring that documents are filed accurately in a timely manner.
- In addition when cover is used they will be properly supervised to ensure the quality of the filing.
- From January 2017 LSBU will be rolling out electronic timesheets and expense claims. This will reduce the amount of paper documentation that has to be retained.

Responsible person/title:

Denise Sullivan, Head of Payroll and Pensions

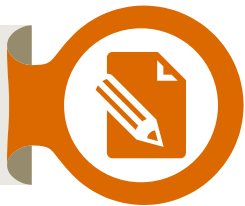
Target date:

30/09/2016

Reference number:

P1

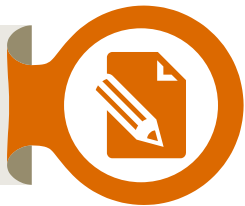
Detailed Findings



Accounts Payable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AP1 Authorised documentation must be received prior to the creating a new or amending a supplier record.	●		●	●	●
AP2 Invoices are approved for payment by an appropriately authorised individual.	●		●	●	●
AP3 Invoices are matched to purchase orders for all expenditure prior to payment and variances investigated.	●		●	●	●

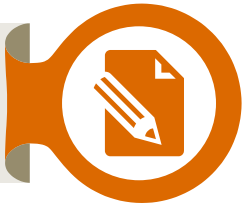
Detailed Findings



Accounts Payable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AP4 BACS payment runs are reviewed by the Financial Controller prior to payment, with all invoices over £10,000 checked to supporting documentation.	●		●	●	●
AP5 Agresso does not allow duplicate suppliers.	●	<ul style="list-style-type: none"> For 2/25 new suppliers, there was no evidence that a check had been performed to confirm the suppliers existence prior to being set up on the system. <p>Management response:</p> <p>Supplier requests are usually approved in batches by a Category Manager but this had not been carried out prior to the audit. This is addressed in control design 2.</p> <p>Responsibility for action:</p> <p>Penny Green, Head of Procurement Services</p>	●	●	●

Detailed Findings



Accounts Payable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AP6 Daily reconciliations are performed between the general ledger and the creditors control accounts. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	●		●	●	●

Validation of Changes to Supplier Details

Control Design

2

Page 140

Finding rating

Rating

Medium risk

Findings

New suppliers and amendments to supplier details are validated after they are processed on the accounts payable system.

LSBU have also not defined when these checks should be performed. We found:

- 1/25 new suppliers sampled was not validated for 38 days after being processed in the accounts payable system.
- 15/20 amendments tested were not validated for over one month. One of these was not validated until 90 days after the change was made in the accounts payable system.

Implications

If supplier information is not validated before a new supplier is added or changes, LSBU may find that invalid suppliers are created or supplier standing data is incorrect. This could lead to inaccurate or fraudulent payments.

If LSBU does not define a time period for retrospective checks to be performed then checks may not be performed for a significant period. This increases the risk of errors not being identified or rectified on a timely basis.

Action plan

The Procurement team will amend this process in the future to ensure that both new suppliers and amendments are validated in a timely manner.

Responsible person/title:

Penny Green, Head of Procurement Services

Target date:

31/10/2016

Reference number:

AP1

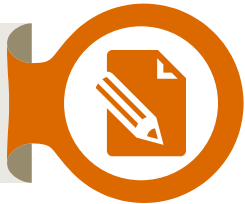
Detailed Findings



Accounts Receivable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AR1 Credit checks are performed on new customer accounts upon request, prior to the commitment of service.	●		●	●	●
AR2 Invoices are properly authorised on Agresso in line with the authorised signatory register.	●		●	●	●

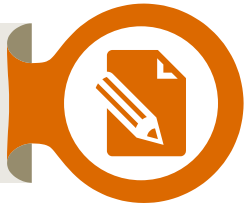
Detailed Findings



Accounts Receivable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AR3 Commercial debt: reminder letters are sent to debtors 30, 60 and 90 days following the invoice issue date in respect of invoiced debt.	●	<ul style="list-style-type: none"> For 2/20 outstanding debts tested, the debt chasing procedure had not been followed. <p>Management response:</p> <p>The process will be revised to link actions with severity of the debt, referral meetings, putting accounts on hold and improved processes for identifying debts that need to be referred to our debt collection agency. This will ensure it is clear what action should be taken at each stage.</p> <p>Responsibility for action:</p> <p>Julian Rigby, Head of Financial Processing</p>	●	●	●
AR4 Student debt: reminder letters are sent in respect of overdue fees on a monthly basis in line with policy.	●		●	●	●

Detailed Findings



Accounts Receivable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AR5 Debts are written off following appropriate review and authorisation.	●		●	●	●
AR6 Monthly reconciliations are performed between the debtors balance on the general ledger and QLX.	●		●	●	●

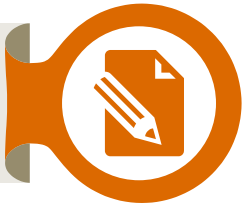
Detailed Findings

Accounts Receivable

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
AR7 Monthly reconciliations are performed between the debtors balance per QLX to QLS.	●		●	●	●
AR8 Monthly reconciliations are performed between the General Ledger and the debtors control accounts. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	●		●	●	●



Detailed Findings



Cash

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
C1 Cash takings in respect of tuition fees and student residences as recorded on QLX and KX are reconciled to cash balances held on a daily basis and discrepancies investigated.	●	<ul style="list-style-type: none"> 1/25 cash banking forms could not be located. <p>Management response: During the period we began storing banking forms electronically and in this instance an incorrect document was filed. To avoid this happening again paper documents will only be destroyed once all transactions are checked and the journal posted correctly to Agresso.</p> <p>Responsibility for action: Vic Van Rensberg, Income Team Leader</p>	●	●	●
C2 Cash deposits made by Loomis are reconciled to records of cash takings on a daily basis.	●		●	●	●

Detailed Findings



Cash

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
C3 Cash receipting responsibility within the QLX system and KX system is restricted to appropriate individuals.	●		●	●	●
C4 Reconciliations are performed on a monthly basis between Agresso and the Bank Statement. These are performed by Treasury Team and reviewed on a timely basis (by the Financial Accountant), with supporting documentation. Reconciling items are investigated on a timely basis.	●		●	●	●

Detailed Findings

General Ledger

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
GL1 Journals must be authorised, with supporting documentation, prior to being posted on the system.	●		●	●	●
GL2 On a monthly basis management accounts are prepared and significant variances against budget are investigated.	●		●	●	●
GL3 Suspense accounts are cleared or reconciled on a quarterly basis.	●		●	●	●



Detailed Findings

General Ledger



Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
GL4 Balance sheet control accounts are cleared or reconciled on a monthly basis.	●	<ul style="list-style-type: none"> 7/25 reconciliations were not prepared on a monthly basis and instead were completed once at year end. 1/25 reconciliations were not dated when reviewed so we cannot confirm if the review took place in a timely manner. 2/25 reconciliations were not been authorised. <p>Management response:</p> <p>The accounts which were not reconciled had zero balances or no movement since year end and staff changes meant that some reconciliations were not authorised during the handover period. There is now a monthly check list in place which will be used to evidence that all balance sheet accounts have been reviewed monthly. The monthly checklist will also be used to ensure that all reconciliations are signed, dated and authorised in a timely manner</p> <p>Responsibility for action:</p> <p>Rebecca Warren/Sally Black, Financial Accountants</p>	●	●	●

Detailed Findings



General Ledger

Key Control	Exceptions P1 2016/17	Details on exceptions	Exceptions P2 2015/16	Exceptions P1 2015/16	Exceptions P3 2014/15
GL5 Access to the general ledger is restricted to appropriate personnel.	●		●	●	●
GL6 No single individual has access to make changes to both the QLX and QLS systems.	●		●	●	●

Retrospective Approval of Journals

Control Design

Page 150

3

Finding rating

Rating

Medium Risk

Findings

Manual journals are approved retrospectively in batches as opposed to being authorised prior to being posted on the system.

Implications

- Invalid, incomplete or inaccurate journals may be posted in the system.
- Fraudulent entries may not be detected by issues identified with the reconciliations may not be identified on a timely basis, leading to further issues.

Action plan

An analysis of the types of transactions posted using unapproved journals is being prepared and the general ledger journal guidance updated to ensure that unapproved journal types are used appropriately. This will reduce the volume of transactions that are approved retrospectively and reduce the risk of invalid or inaccurate journals being posted.

Responsible person/title:

Natalie Ferer, Financial Controller

Target Date:

30/11/2016

Reference number:

GL1

Budget Variances

Control Design

4

Page 151

Finding rating

Rating

Advisory

Findings

On a monthly basis management accounts are prepared and significant variances against budget are investigated but there is no defined threshold for what constitutes a ‘significant’ variance against budget.

Implications

There may be an inconsistent approach to investigating variances month on month. Significant or unusual variances may not be investigated.

Action plan

This recommendation has not been implemented. The process will be reviewed and updated to ensure that there is a consistent approach to investigating variances.

Responsible person/title:

Ralph Sanders, Financial Planning Manager

Target date:

30/11/2016

Reference number:

GL2

**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

Appendices

Page 152

Appendix A: Basis of our classifications

System summary ratings

The finding ratings in respect of each financial sub-process area are determined with reference to the following criteria.

Rating	Assessment rationale
● Red	A high proportion of exceptions identified across a number of the control activities included within the scope of our work; or Control failures which, individually or in aggregate, have resulted in the significant misstatement of the University's financial records.
● Amber	Some exceptions identified in the course of our work, but these are limited to either a single control or a small number of controls; or Control failures which, individually or in aggregate, have resulted in the misstatement of the organisations financial records, but this misstatement is not significant to the University
● Green	Limited exceptions identified in the course of our work Control failures which, individually or in aggregate, do not appear to have resulted in the misstatement of the organisations financial records.

Control design improvement classifications

The finding ratings in respect of each financial sub-process area are determined with reference to the following criteria.

Critical

A finding that could have a:

- **Critical** impact on operational performance resulting in inability to continue core activities for more than two days; or
- **Critical** monetary or financial statement impact £5m; or
- **Critical** breach in laws and regulations that could result in material fines or consequences over £500k; or
- **Critical** 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.

Appendix A: Basis of our classifications

High

A finding that could have a:

- **Significant** impact on operational performance resulting in significant disruption to core activities; or
- **Significant** monetary or financial statement impact of £2m; or
- **Significant** breach in laws and regulations resulting in significant fines and consequences over £250k; or
- **Significant** impact on the reputation or brand of the organisation, resulting in unfavourable national media coverage.

Medium

Page 154

A finding that could have a:

- **Moderate** impact on operational performance resulting in moderate disruption of core activities or significant disruption of discrete non-core activities; or
- **Moderate** monetary or financial statement impact of £1m; or
- **Moderate** breach in laws and regulations resulting in fines and consequences over £100k; or
- **Moderate** impact on the reputation or brand of the organisation, resulting in limited unfavourable media coverage.

Low

A finding that could have a:

- **Minor** impact on the organisation's operational performance resulting in moderate disruption of discrete non-core activities; or
- **Minor** monetary or financial statement impact of £500k; or
- **Minor** breach in laws and regulations with limited consequences over £50k; or
- **Minor** impact on the reputation of the organisation, resulting in limited unfavourable media coverage restricted to the local press.

Advisory

A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Appendix B: Terms of reference

Continuous Auditing: Key Financial Systems

2016/17

To: Richard Flatman – Chief Financial Officer
From: Justin Martin – Head of Internal Audit

Page 155

Background and audit objectives



This review is being undertaken as part of the 2016/2017 internal audit plan approved by the Audit Committee.

Background and audit objectives

The purpose of our Continuous Audit programme is to test key controls on an on-going basis to assess whether they are operating effectively and to flag areas and/or report transactions that appear to circumvent controls. Testing is undertaken twice a year and provides the following benefits:

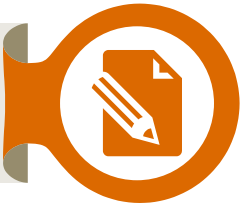
- It provides management with an assessment of the operation of key controls on a regular basis throughout the year;
- Control weaknesses can be addressed during the year rather than after the year end; and
- The administrative burden on management will be reduced when compared with a full system review, in areas where there is sufficient evidence that key controls are operating effectively.

We have outlined the specific controls we will be testing in Appendix 1. These have been identified through our annual audit planning process and meetings with management to update our understanding of the control framework in place. We will continue to refresh this knowledge throughout the year to ensure we focus upon the key risks facing London South Bank University (LSBU). Where the control environment changes in the financial year or we agree with management to revise our approach, we will update Appendix 1 and re-issue our Terms of Reference.

Our work touches upon the following areas that form part of our annual report to Audit Committee:

Total plan days	Financial Control	Value for Money	Data Quality	Corporate Governance	Risk management	
25	x	x	x	x	x	x = area of primary focus x = possible area of secondary focus

Audit scope and approach (1 of 4)



Scope

The financial processes, key control objectives and key risk areas included within the scope of this review are:

Sub-process	Key Control Objectives	Key risks
Payroll and staff expenses	<p>Accurate payments are made to valid employees of the organisation.</p> <p>Accurate payments are made in respect of valid expenses claims.</p>	<ul style="list-style-type: none"> Fictitious employees are established on the payroll and/or employees are established on the payroll incorrectly (e.g. incorrect pay scale). Payments are made in error to employees who have left the organisation and / or inaccurate final salary payments are made. Overtime or other timesheet based records are inaccurate leading to salary over / under payments. Invalid changes are made to employee salary and bank details leading to incorrect salary payments being made. Information transferred from the payroll system to the main accounting system is not complete and accurate. Expenses are incurred and reimbursed that are not allowable.

Audit scope and approach (2 of 4)

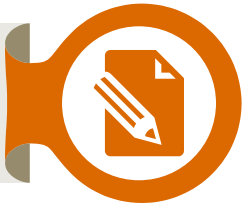


Scope

The financial processes, key control objectives and key risk areas included within the scope of this review are:

Sub-process	Key Control Objectives	Key risks
Accounts payable	<p>Expenditure commitments are made with prior budgetary approval.</p> <p>Payments are made only following the satisfactory receipt of goods or services.</p> <p>Payments are made only to valid suppliers.</p>	<ul style="list-style-type: none"> • Payments are made for goods and services which have not been ordered, received or are inadequate. • Invalid suppliers or supplier standing data is maintained leading to inaccurate or fraudulent payments. • Information transferred from the accounts payable system to the main accounting system is not complete and accurate. • Amounts due to suppliers for goods and services are overpaid.
Accounts receivable	<p>Fee income is collected on a timely basis.</p> <p>Goods or services are delivered only to credit worthy customers.</p> <p>Debts due are collected promptly.</p>	<ul style="list-style-type: none"> • Agreements are entered in to with customers prior to the performance of credit checks or credit limits are exceeded. This may mean debts are not recoverable. • Overdue debtor balances are not identified and balances are not actively chased to ensure timely collection of debts and maximisation of income. • Information transferred from the accounts receivable system to the main accounting system is not complete and accurate.

Audit scope and approach (3 of 4)



Scope

The financial processes, key control objectives and key risk areas included within the scope of this review are:

Sub-process	Key Control Objectives	Key risks
Cash	Cash ledger balances are accurate and complete. Cash is not lost or misappropriated.	<ul style="list-style-type: none"> Information transferred from the cash receipting systems to the main accounting system is not complete and accurate Discrepancies between the ledger and till or float records are not promptly identified and investigated. This could mean cash balances are incomplete and / or inaccurate.
General Ledger	Ledger balances are valid and accurate.	<ul style="list-style-type: none"> Invalid, incomplete or inaccurate journals are posted. This could disguise misappropriations or mean there is no evidence to support decisions made. Suspense accounts and balance sheet control accounts are not cleared on a timely basis. Segregation of duties is not maintained, this could compromise the validity and accuracy of general ledger information.

Audit scope and approach (4 of 4)



Limitations of scope

Our work is not intended to provide assurance over the effectiveness of all the controls operated by management over these financial systems; the focus of our work will be limited to those controls which are deemed by management to be most significant to the system under consideration.

Our work will not consider the organisations IT security framework and associated controls in place.

Audit approach

We will undertake our testing twice a year, covering the following periods during 2016/17:

- Phase 1: January 2016 – July 2016
- Phase 2: August 2016 – December 2016



Internal audit team



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@uk.pwc.com
Charlotte Bilsland	Engagement Senior Manager	07715 484 470 charlotte.bilsland@uk.pwc.com
Lucy Gresswell	Engagement Supervisor	07718 098 321 lucy.j.gresswell@uk.pwc.com
Janak Savjani	Continuous Auditing Technician	07802 660 974 janak.j.savjani@uk.pwc.com
Richard Bettles	Continuous Auditing Technician	07841 787 852 richard.d.bettles@uk.pwc.com



Key contacts

Key contacts – London South Bank University

Name	Title	Contact details	Responsibilities
Richard Flatman	Chief Financial Officer (Audit Sponsor)	0207 815 6301 richard.flatman@lsbu.ac.uk	Review and approve terms of reference Review draft report
John Baker	Corporate and Business Planning Manager	0207 815 6003 j.baker@lsbu.ac.uk	Review and approve final report
Natalie Ferer	Financial Controller	0207 815 6316 ferern@lsbu.ac.uk	Hold initial scoping meeting Review and meet to discuss issues arising and develop management responses and action plan
Joanne Monk	Deputy Director of Human Resources	j.monk@lsbu.ac.uk	Audit contact
Jenny Laws	Deputy Registrar (Student Management Information Team Leader)	lawsjr@lsbu.ac.uk	Audit contact
Ralph Sanders	Financial Planning Manager	sanderr4@lsbu.ac.uk	Audit contact
Brian Wiltshire	Payments Manager	wiltshbl@lsbu.ac.uk	Audit contact
Penny Green	Head of Procurement	greenp7@lsbu.ac.uk	Audit contact

Key contacts



Key contacts – London South Bank University

Name	Title	Contact details	Responsibilities
Julian Rigby	Head of Financial Processing	rigbyj@lsbu.ac.uk	Audit contact
Ravi Mistry	Financial Systems Manager	mistryrm@lsbu.ac.uk	Audit contact
Denise Sullivan	Payroll Manager	d.sullivan@lsbu.ac.uk	Audit contact
Rebecca Warren	Financial Accountant	warrenra@lsbu.ac.uk	Audit contact
Andrew Ratajczak	Manager; Fees, Bursaries and Central Enrolment	ratajca@lsbu.ac.uk	Audit contact

Timetable



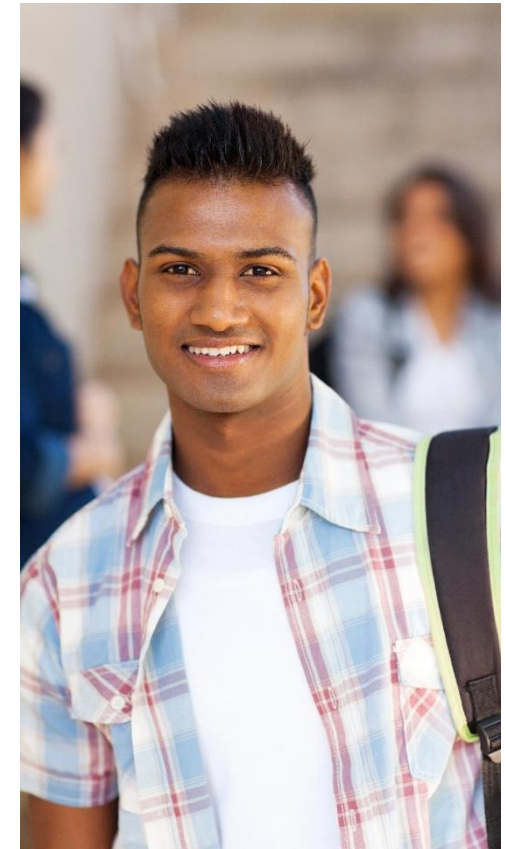
Timetable

	Phase 1	Phase 2
Fieldwork start	22/08/2016	16/01/2017
Fieldwork completed	26/08/2016	27/01/2017
Draft report to client	02/09/2016	10/02/2017
Response from client	09/09/2016	24/02/2017
Final report to client	16/09/2016	03/03/2017

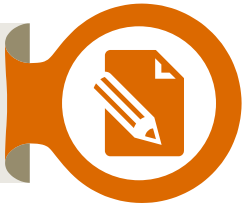
Agreed timescales are subject to the following assumptions:

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

Please note that if the University requests the audit timing to be changed at short notice (2 weeks before fieldwork start) and the audit staff cannot be deployed to other client work, the University may still be charged for all/some of this time. PwC will make every effort to redeploy audit staff in such circumstances.



Appendix 1: Key controls schedule



Based upon our understanding of the financial systems in place at LSBU and in discussion with management, we have agreed that the operating effectiveness of the following controls will be considered. These have been mapped to the key risks identified as in scope above.

Payroll

Key Contacts: Denise Sullivan and Joanne Monk

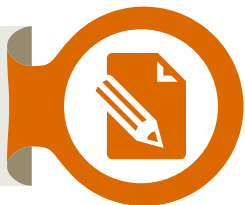
Key risk	Key Control	Reference
Fictitious employees are established on the payroll and/or employees are established on the payroll incorrectly (e.g. incorrect pay scale)	Authorised and accurate new starter forms are received prior to an individual being entered on to the payroll system.	P1
Payments are made in error to employees who have left the organisation and / or inaccurate final salary payments are made	Leaver forms are received from Human Resources upon notification of resignation or redundancy.	P2
	The BACS run is reviewed by the Financial Controller and a Payment Release Form completed.	P3

Appendix 1: Key controls schedule



Key risk	Key Control	Reference
Payments are made in error to employees who have left the organisation and / or inaccurate final salary payments are made	<p>The following exception reports are produced and reviewed as part of month-end procedures, before the payment run is authorised:</p> <ul style="list-style-type: none"> • Errors and warnings reports (i.e. processing issues encountered); • Payroll differences (difference between each element between two periods, with tolerances of between 5% and 10%); • Gross pay over £6,000; • Number of staff paid in comparison to previous month with subsequent reconciliation; • Starters and leavers for the period; • Element differences between two periods for overtime and bonuses; and • HMRC payments. 	P4
Invalid changes are made to employee salary and bank details leading to incorrect salary payments being made	Variation forms, with supporting documentation, are received prior to any changes being made to standing data.	P5
	Access to the payroll system is restricted to appropriate personnel.	P6
Overtime or other timesheet based records are inaccurate leading to salary over / under payments	Appropriately authorised overtime claim forms and timesheets are received prior to payment being made.	P7

Appendix 1: Key controls schedule



Key risk	Key Control	Reference
Information transferred from the payroll system to the main accounting system is not complete and accurate	Monthly reconciliations are performed between the general ledger and the payroll system. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	P8
Expenses are incurred and reimbursed that are not allowable	Expenses are supported by appropriately authorised claim forms.	P9

Accounts Payable

Key Contacts: Brian Wiltshire, Penny Green, Rob Ager, Ravi Mistry (AP1) and Maureen Stanislaus (AP2 – AP6)

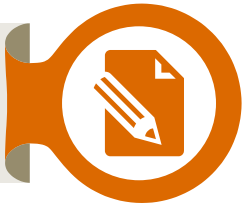
Key risk	Key Control	Reference
Invalid suppliers, or supplier standing data, is maintained leading to inaccurate or fraudulent payments	Authorised documentation must be received prior to the creating a new or amending a supplier record.	AP1
Payments are made for goods and services which have not been ordered, received or are inadequate. Invoices payments are not appropriately reviewed and authorised prior to payment	Invoices are approved for payment by an appropriately authorised individual	AP2
	Invoices are matched to purchase orders for expenditure prior to payment and variances investigated.	AP3

Appendix 1: Key controls schedule



Key risk	Key Control	Reference
Payments are made for goods and services which have not been ordered, received or are inadequate. Invoices payments are not appropriately reviewed and authorised prior to payment	BACS payment runs are reviewed by the Financial Controller prior to payment, with all invoices over £10,000 checked to supporting documentation.	AP4
Amounts due to suppliers for goods and services are over paid	Agresso does not allow duplicate suppliers.	AP5
Information transferred from the accounts payable system to the main accounting system is not complete and accurate	Daily reconciliations are performed between the general ledger and the creditors control accounts. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	AP6

Appendix 1: Key controls schedule



Accounts Receivable

Key Contacts: Natalie Ferer, Vic Van Rensburg, Julian Rigby and Ian Macleay

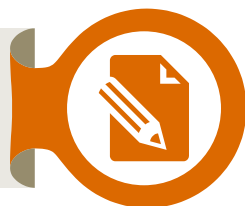
Key risk	Key Control	Reference
Agreements are entered into with customers prior to the performance of credit checks or credit limits are exceeded. This may mean debts are not recoverable.	Credit checks are performed on new customer accounts upon request, prior to the commitment of service.	AR1
Overdue debtor balances are not identified and balances are not actively chased to ensure timely collection of debts and maximisation of income	Invoices are properly authorised on Agresso in line with the authorised signatory register.	AR2
	Commercial debt: reminder letters are sent to debtors 30, 60 and 90 days following the invoice issue date in respect of invoiced debt.	AR3
	Student debt: reminder letters are sent in respect of overdue fees on a monthly basis in line with policy.	AR4
	Debts are written off following appropriate review and authorisation.	AR5

Appendix 1: Key controls schedule



Key risk	Key Control	Reference
Information transferred from the accounts receivable system and student record system to the main accounting system is not complete and accurate	Monthly reconciliations are performed between the debtors balance on the general ledger and QLX.	AR6
	Monthly reconciliations are performed between the debtors balance per QLX to QLS.	AR7
	Monthly reconciliations are performed between the General Ledger and the debtors control accounts. These are prepared and reviewed on a timely basis, with supporting documentation. Reconciling items are investigated on a timely basis.	AR8

Appendix 1: Key controls schedule



Cash

Key Contacts: Vic Van Rensburg, Julian Rigby and Brian Wiltshire (C4)

Key risk	Key Control	Reference
Information transferred from the cash receipting systems to the main accounting system is not complete and accurate	Cash takings in respect of tuition fees and student residences as recorded on QLX and KX are reconciled to cash balances held on a daily basis and discrepancies investigated.	C1
Discrepancies between the ledger and till or float records are not promptly identified and investigated. This could mean cash balances are incomplete and / or inaccurate	Cash deposits made by Loomis are reconciled to records of cash takings on a daily basis.	C2
	Cash receipting responsibility within the QLX system and KX system is restricted to appropriate individuals.	C3
	Reconciliations are performed on a monthly basis between Agresso and the Bank Statement. These are performed by the Financial Accounting Team and reviewed on a timely basis (by the Financial Accountant), with supporting documentation. Reconciling items are investigated on a timely basis.	C4

Appendix 1: Key controls schedule



General Ledger

Key Contacts: Rebecca Warren (GL1, GL3, GL4), Ralph Sanders (GL2), Ravi Mistry (GL5, GL6)

Key risk	Key Control	Reference
Invalid, incomplete or inaccurate journals are posted. This could disguise misappropriations or mean there is no evidence to support decisions made	Journals must be authorised, with supporting documentation, prior to being posted on the system.	GL1
	On a monthly basis management accounts are prepared and variances against budget are investigated. The following thresholds are applied at an account code level for investigation: <ul style="list-style-type: none"> • ≥ 10% variance between actuals and the budget or forecast where the total variance greater than £10,000 • ≥ £100,000 variance between actuals and the budget or forecast. 	GL2
Suspense accounts and balance sheet control accounts are not cleared on a timely basis	Suspense accounts are cleared or reconciled on a quarterly basis.	GL3
	Balance sheet control accounts are cleared or reconciled on a monthly basis.	GL4
Segregation of duties is not maintained, this could compromise the validity and accuracy of general ledger information	Access to the general ledger is restricted to appropriate personnel.	GL5
	No single individual has access to make changes to both the QLX and QLS systems.	GL6

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. 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.

Future periods

Our assessment of controls is for the period specified only. 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 changes; or
- The degree of compliance with policies and procedures may deteriorate.

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 endeavour to plan our work so that we have a reasonable expectation of detecting significant control weaknesses and, if detected, we 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.

This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

Internal audit work was performed in accordance with PwC's Internal Audit methodology which is aligned to the Memorandum of Assurance and Accountability (MMA) between Higher Education Funding Council for England (HEFCE) and institutions. 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.

In the event that, pursuant to a request which London South Bank University has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), London South Bank University is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such report. If, following consultation with PwC, London South Bank University discloses any this document 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.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

	CONFIDENTIAL
Paper title:	Internal Audit Annual Report: 2015/16
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with the Internal Audit Annual Report for 15/16.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	The internal audit plan relates to controls and processes that relate to the entire organisation, and provide assurance against all of the risk types within the Corporate Risk Appetite statement.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Matter previously considered by:		On:
Further approval required?		

Executive Summary

The internal audit annual report is part of the annual accountability return we make to Hefce, and contains the opinion which is included in the published accounts.

The opinion within this report for 2015/16 is “generally satisfactory with some improvements required”. This is consistent with the previous year, and the second highest of four potential categories.

The commentary on page two highlights these areas, which mainly relate to the IT environment.

The table of findings on page seven demonstrates that overall, the numbers of findings in 15/16 have reduced when compared to the previous year. 88% of agreed actions have been implemented in year which is ahead of benchmark target (75%) and the 14/15 total (78%).

- The Committee is requested to note the annual report.

*Internal Audit
Annual Report
2015/2016*
DRAFT

**London South
Bank University**
September 2016

Contents

1. Executive summary	1
2. Summary of findings	3
3. Internal Audit work conducted	6
4. Follow up work conducted	11
<hr/>	
Appendices	12
Appendix 1: Limitations and responsibilities	13
Appendix 2: Opinion types	14
Appendix 3: Basis of our classifications	15
Appendix 4: Outstanding Recommendations	17
Appendix 5: Mapping of internal audit work	19

Distribution List

For action	Richard Flatman, Chief Financial Officer Audit Committee
For information	James Stevenson, University Secretary

This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University under our contract dated 15/05/2015.

1. Executive summary

Introduction

This report outlines the internal audit work we have carried out for the year ended 31/07/2016.

The Higher Education Funding Council for England's (HEFCE) Memorandum of Assurance and Accountability (MAA) requires that the Head of Internal Audit provides a written report and annual internal audit opinion to the Audit Committee. The purpose of this report is to present our view on the adequacy and effectiveness of:

- Governance, risk management and control; and
- Economy, efficiency and effectiveness (value for money) arrangements.

This is achieved through a risk-based plan of work, agreed with management and approved by the Audit Committee, which should provide a reasonable level of assurance, subject to the inherent limitations described below and set out in Appendix 1. The opinion does not imply that Internal Audit has reviewed all risks relating to the organisation.

The Audit Committee agreed to a level of internal audit input of 125 days, of which 123 days were delivered. Whilst this report is a key element of the framework designed to inform the Audit Committee's Annual Report to HEFCE, there are also a number of other important sources to which the Audit Committee should look to gain assurance. This report does not override the Audit Committee's responsibility for forming their own view on governance, risk management, control and value for money arrangements.

Head of Internal Audit Opinion

We are satisfied that sufficient internal audit work has been undertaken to allow an opinion to be given as to the adequacy and effectiveness of governance, risk management and control, and economy, efficiency and effectiveness arrangements (value for money). To assist the Audit Committee in understanding how our work corresponds to their reporting responsibilities, we have mapped our work against these areas in Appendix 5.

In giving this opinion, it should be noted that assurance can never be absolute. The most that the internal audit service can provide is reasonable assurance that there are no major weaknesses in the system of internal control.

Opinion

Our opinion is as follows:

Satisfactory	Generally satisfactory with some improvements required	Major improvement required	Unsatisfactory
--------------	---	----------------------------	----------------

Governance, risk management and control, and value for money arrangements in relation to business critical areas is generally satisfactory. However, there are some areas of weakness in the framework of governance, risk management and control and value for money arrangements which potentially put the achievement of objectives at risk.

Improvements are required in those areas to enhance the adequacy and effectiveness of governance, risk management and control and value for money arrangements. Please see our Summary of Findings in Section 2.

An explanation of the types of opinion that may be given can be found in Appendix 2.

Basis of opinion

Our opinion is based on:

- All audits undertaken during the year.
- Any follow up action taken in respect of audits from previous periods.
- Any significant recommendations not accepted by management and the resulting risks.
- The effects of any significant changes in the organisation's objectives or systems.

The commentary below provides the context for our opinion and together with the opinion should be read in its entirety.

Commentary

The key factors that contributed to our opinion are summarised as follows:

- Our view on London South Bank University's operational control environment and governance arrangements is underpinned by the audit reviews that we have performed during the year. There has been one high risk rated report, two medium risk rated reports and two low risk rated reports prepared during the financial year. The findings from these reports are not considered significant in aggregate to the system of internal control. None of the individual assignments completed in 2015/16 have an overall classification of critical risk.
- We note that the strength of control and governance of London South Bank University's IT environment continues to be an area which requires management focus. Our Information Security review has been classified as high risk for 2015/16; this review was also classified as high risk in both our 2013/14 and 2014/15 Annual Opinion. While our risk rating is consistent with prior year, we recognise that a significant amount of work has been done to update and rationalise the IT controls in place and improvements have been made.
- In addition to our Information Security report, we performed a specialist review over the external infrastructure. This review identified six recommendations required to mitigate the risk of an external malicious attack. Our work found that London South Bank University is running unsupported and outdated software on services visible over the internet; this exposes the infrastructure to attacks and could potentially compromise those services. We note that management directed us to look at this area because it was a known risk to the organisation and this has helped form our opinion that while these findings are not indicative of systematic threats to the entire control and governance environment, they do suggest that the IT control environment needs to be strengthened.
- London South Bank University's risk management arrangements continue to be strong as evidenced by our low risk report on Risk Management. The risk management approach integrates risk management with the strategic and business planning process; this is in line with good practice, as many of the institutions included in our 2016 Risk Management Benchmarking Exercise did not align risks to corporate objectives. This will help to ensure resources are directed at the highest priority risks and are managed efficiently and effectively.
- Our Continuous Auditing work shows that on the whole the core financial control environment has remained robust during the year with no significant exceptions or control recommendations raised. Performance has slightly declined towards the end of the year; untimely preparation and authorisation of reconciliations is a recurring theme, affecting Payroll and General Ledger. We have also continued to see exceptions affecting starter and leaver documentation within Payroll, which was either missing or has not been authorised on a timely basis.
- The timely implementation of internal audit recommendations by management is a key indicator of good governance and a target rate of 75%+ should be aspired to by management. London South Bank University's implementation rate has improved in 2015/16; 88% of agreed actions have been implemented compared to 78% in the 2014/15.
- Our work over value for money indicates that the processes in place to ensure value for money is achieved are in accordance with good practice, for example: adherence to financial controls and use of purchase consortiums.

Acknowledgement

We would like to take this opportunity to thank London South Bank University staff, for their co-operation and assistance provided during the year.

2. Summary of findings

Our annual internal audit report is timed to inform the organisation's Audit Committee's Annual Report to HEFCE

A summary of key findings from our programme of internal audit work for the year work is recorded in the table below:

Description	Detail
<p>Overview</p> <p>We completed 9 internal audit reviews. This resulted in the identification of 0 critical, 2 high, 15 medium and 3 low risk findings to improve weaknesses in the design of controls and / or operating effectiveness.</p> <p>The total number of findings has decreased from 26 in 2014/15 to 20. Given this background, the results suggest that London South Bank University has managed to retain a stable control environment.</p> <p>Both of the two high risk findings were isolated to the Information Security review. We have outlined this in more detail in the section below.</p>	<p>Our audit plan was scoped to address London South Bank University's key risks and strategic objectives. We mapped each review to these areas in our Internal Audit Risk Assessment and Internal Audit Plan 2015/16.</p> <p>We have completed our Internal Audit Plan in line with the set timescales.</p>
<p>Risk Management, Control and Governance</p> <p>Risk Management:</p> <p>Risk management arrangements remain strong with a number of areas of good practice.</p> <p>Our report was rated low risk which represents a positive direction of travel for the institution. The review identified just one medium risk finding, which relates to ensuring that organisational risk registers are regularly updated and fully completed.</p> <p>Control:</p> <p>The results of our Key Financial Systems Continuous Auditing has remained largely consistent throughout the year. Although we did identify two medium risk findings in the second phase of 2015/16:</p> <ul style="list-style-type: none"> We found that payroll paper work was not being filed on a timely basis, resulting in difficulty locating some key documents; and Some manual journals are being retrospectively approved after being posted in the general ledger. <p>A summary of Continuous Auditing performance and the results of individual reviews is included in Section 3. The overall performance of financial controls compliance has remained strong in 2015/16.</p> <p>Our work on Information Security suggests that the IT control environment continues to be a high risk. We identified two high risk findings which have been summarised opposite.</p>	<p>Information Security – high risk findings</p> <p>User Administration</p> <ul style="list-style-type: none"> There is no communication with IT when changes are required to a user's AD account. We understand from discussion with management that changes made are additive, meaning that staff moving may retain access to data they are no longer permitted to see. We were unable to obtain a listing of modifications to AD accounts. We found that four of the 30 leavers tested still had active AD accounts at the date of fieldwork. <p>Logical Security</p> <ul style="list-style-type: none"> A number of findings were identified due to weaknesses in the controls over encrypting devices: USB's, mobile devices, desktops and laptops. Password parameters were found to be incorrectly set-up. <p>External Infrastructure</p> <ul style="list-style-type: none"> Our specialist review of external infrastructure identified six actions for management to implement in order to protect against the threat of an external malicious attack. The most significant findings were in relation to unsupported and outdated software which leaves London South Bank University vulnerable to an external attack and data breach.

<p>As part of this work we performed a specialist review on the external infrastructure which has identified a number of key priorities for London South Bank University to take forward. These findings have also been summarised opposite.</p> <p>Governance:</p> <p>Our core financial systems work has identified appropriate segregation of duties and reporting / documenting of key processes and there have been no significant issues raised as part of individual reviews performed.</p>	
<p>Value for Money</p> <p>Institutions have a duty of care to ensure the proper use of public funds and the achievement of value for money. Our audit approach considers value for money as an integral objective of London South Bank University's systems of internal control. Our work indicates that London South Bank University has processes in place to ensure value for money which are in accordance with good practice, examples are provided opposite.</p>	<p>Value for money has been demonstrated through the following activities:</p> <ul style="list-style-type: none"> • Use of purchasing consortiums – London South Bank University are a member of the London Universities Purchasing Consortia; • Adherence to financial controls - as part of our Continuous Auditing work we test to ensure transactions are approved and reviewed in accordance with London South Bank University's delegated authority framework. No significant issues have been noted this year; and • Value for Money Working Group – a working group was established in 2013 and is attended by senior officers across the organisation. This also focuses on delivering value for money for students.
<p>Data Quality</p> <p>The MAA includes a mandatory requirement for quality assurances to be provided by Institutions over the data submitted to the Higher Education Statistics Agency (HESA) and HEFCE.</p> <p>Whilst there is no requirement for our internal audit programme to provide a conclusion in respect of data quality, our internal audit programme in 2015/16 has been designed to support the Audit Committee in forming its conclusion in respect of such matters.</p>	<p>Continuous Auditing</p> <p>The two Student Data Continuous Auditing reports issued in 2015/16 were both classified as low risk. We have not identified any significant exceptions regarding student data controls, but in the second phase of fieldwork we identified an increase in the number of exceptions which suggests that there has been a deterioration in performance. This should be monitored by management to ensure that this remains low risk.</p> <p>Management Information: Data Quality</p> <p>We identified four medium and one low risk rated finding in this review. The medium risks related to:</p> <ul style="list-style-type: none"> • Missing and inaccurate data used for three of the five KPI's tested. • Supporting evidence (i.e. telephone surveys) could not be located for 17 of the 25 students sampled in our testing over graduate employment KPI's. • There was no data collection methodology in place. • Guidance for data quality differed between policy documents.

Good practice

We also identified a number of areas where few weaknesses were identified and / or areas of good practice.

Prevent Duties

- We completed a review on London South Bank University's response to the Government's Prevent Strategy and provisions in the Counter-Terrorism and Security Act 2015. We noted that London South Bank University has been proactive in their response to Prevent, including consulting with HEFCE and members of the London Higher Education Prevent Network and has been advising other University's on best practice.

Research and Enterprise Contracts

- We conducted a review over the design of London South Bank University's new policy and procedure for enterprise income, covering the process up to contract signature. We also tested the procedures for ensuring compliance with research grant terms and conditions, post-award.
- We noted that the new policy for enterprise income introduced a well-defined and standardised process for entering into new contracts. We found no exceptions in this area of the review and concluded that the procedure document is robust.

Risk Management

- Risk Management arrangements remain strong with a number of areas of good practice, for example: documented roles and responsibilities, established management escalation routes and a defined Risk Strategy and Risk Appetite.

3. Internal Audit work conducted

Introduction

The table below sets out the results of our internal audit work.

We have also provided an analysis on page 7 of findings identified year on year to provide an indicative direction of travel.

The criteria for our report classifications and the definitions applied in the assessment of our individual findings are included in Appendix 3. We also include a comparison between planned internal audit activity and actual activity on page 10.

Results of individual assignments






Review	Report classification	Report Status	Number of findings			
			Critical	High	Medium	Low
Continuous Auditing: Key Financial Systems – Phase 1	No Classification	Final	-	-	-	-
Continuous Auditing: Key Financial Systems – Phase 2	No Classification	Final	-	-	2	1
Continuous Auditing: Student Data – Phase 1	No Classification	Final	-	-	-	1
Continuous Auditing: Student Data – Phase 2	No Classification	Final	-	-	-	-
Management Information: Data Quality	Medium	Final	-	-	4	1
Research and Enterprise Contracts	Medium	Final	-	-	5	-
Risk Management	Low	Final	-	-	1	-
Prevent	Low	Final	-	-	2	-
Information Security	High	Final	-	2	1	-
		Total	-	2	15	3

Note that the above does not include a specialist review conducted over London South Bank University's external infrastructure. This report was commissioned as part of the Information Security review.

Implications for next year's plan

Information Security continues to be a high risk area for London South Bank University. We have included an IT audit in the 2016/17 Plan.

Direction of control travel

Finding rating	Trend between current and prior year	Number of findings		
		2015/16	2014/15	2013/14
Critical		0	0	0
High		2	4	2
Medium		15	13	8
Low		3	9	8
Total		20	26	18

Implications for management

The overall number of findings has declined which indicates that there has been an improvement in the control environment compared to the previous year. Although the number of medium risk findings have increased by two, the number of high risk rated findings have decreased by two. The number of low risk rated findings have decreased significantly and there remains no critical findings.

The trend should be considered in the context that we conduct different reviews each year which present different risk profiles. In 2014/15 the majority of the 26 findings came from a review on the Change Programme (six medium and three low risk findings). As a result, this one review may distort the performance trend.

Both of the two high risk findings identified in the current year relate to one review: Information Security. This was a known area of risk for London South Bank University, which we were directed towards testing and our results suggest that this continues to be an area requiring management focus.

No classification has been given for four reviews performed, these relate to Continuous Auditing. An analysis of findings in these areas has been provided below. We have provided risk-rated findings where exceptions were noted in our testing. The results of our Continuous Auditing show a slight decline in performance throughout the year (see below). We have not identified any risks which are pervasive to the entire control environment.

Analysis of the Continuous Auditing programme

Whilst no overarching classification is assigned for our Continuous Auditing reports, we have summarised below the findings identified in each period under consideration as part of the 2015/16 audit programme. The comparative performance for 2014/15 is also shown.

Key Financial Systems

The table below represents our view of the overall risk for each system within each financial cycle. The numbers in brackets represents the number of control effectiveness exceptions identified from our work. The control design recommendations identified are summarised within the table included on page 6).

System / Rating	Trend	2016/17 IA Programme		2015/16 IA Programme		2014/15 IA Programme	
		P1 2016/17	P2 2015/16	P1 2015/16	P3 2014/15	P2 2014/15	P1 2014/15
Payroll	↔	● Amber (4)	● Amber (5)	● Green (0)	● Green (2)	● Green (2)	● Green (0)
Accounts Payable	↔	● Green (1)	● Green (0)	● Green (2)	● Green (1)	● Amber (1)	● Green (0)
Accounts Receivable	↔	● Green (1)	● Green (3)	● Green (1)	● Green (2)	● Green (1)	● Green (0)
Cash	↔	● Green (1)	● Green (1)	● Green (0)	● Amber (2)	● Amber (1)	● Green (0)
General Ledger	↓	● Amber (1)	● Green (1)	● Green (1)	● Green (2)	● Green (0)	● Green (0)

Overall there has been a deterioration in performance during this period due to an increase in the number of operating effectiveness and control design exceptions identified. Payroll in particular has moved from a green rating in all previous periods to an amber rating, this has been attributed to filing issues in the payroll team following the recent restructure. Untimely preparation and authorisation of reconciliations is also recurring theme, affecting Payroll and General Ledger.

Student Data

The table below summarises the overall performance for student data this period. This is based on the number and severity of findings noted each period. We classified the overall area as *low risk* in both phases in 2015/16; this was classified as medium risk for both phases in 2014/15.

Control	Trend	2015/16 – P2		2015/16 – P1		2014/15 – P2		2014/15 – P1	
		Effectiveness	Design	Effectiveness	Design	Effectiveness	Design	Effectiveness	Design
S1	↔	6	-	6	-	6	-	-	-
S2	↓	2	-	-	-	1	-	5	-
S3	N/A ⁽¹⁾	-	-	-	-	7	-	4	-
S4	↓	5	-	-	-	3	1	-	-
S5	↑	3	-	7	1	2	1	8	-
S6	↑	-	-	4	-	9	-	3	-
S7	↓	2	-	1	-	-	-	1	-
S8	↓	5	-	-	-	-	-	2	-
S9	↔	-	-	-	-	4	-	1	-
S10	↓	1	-	-	-	1	-	6	-
S11	↑	-	-	1	-	1	-	-	-
S12	N/A ⁽¹⁾	-	-	-	-	1	-	-	-
Total	↓	23	-	18	1	35	2	30	0

Our continuous auditing programme for student data also includes computer assisted audit techniques (CAATS) which we used to perform data mining procedures over a sample of courses and modules to confirm that student timetabling data is correct. The table below summarises the results from our data assurance testing:

Test	Test Detail	Trend	2015/16		2014/15	
			P2 (01/08/2015 – 31/10/2015)	P1 (01/11/2015 – 31/03/2016)	P2 (01/11/2014 – 31/03/2015)	P1 (01/08/2014 – 31/10/2014)
1	We checked that for all instances where a student is in the QLS extract, the student is also enrolled on one of these 5 modules.	↔	-	-	-	1
2	We checked that for all instances where a student is enrolled on a module they are also in the extract taken from QLS.	↓	31	12	19	76
3	We checked that, for all larger modules, there are sub-groupings and that the modules and their sub-groupings contain the same students.	↓	73	33	58	176
4	We checked that, for each course, the students affiliated with the timetable are listed in the QLS extract.	↑	5	8	47	3
5	We checked that, for each course, the students listed in the QLS extract are linked to the course timetable.	↔	2	2	46	1
6	We checked that, for each course, the students not recorded as fully enrolled in the course timetable are not in the QLS extract.	↔	-	-	30	2
Total		↓	111	55	200	259

As can be seen in the two tables above, although the overall area has been classified as low risk for both periods in 2015/16, there have been an increase in the number of exceptions in the second phase of 2015/16.

Implications for next year's plan

We will continue to monitor the performance of payroll in the 2016/17 Key Financial Systems Continuous Audit to verify whether the filing issues have been resolved.

Comparison of planned and actual activity

<i>Audit Unit</i>	<i>Budgeted days</i>	<i>Actual days</i>
Continuous Auditing: Financial Controls – Phase 1 (May to July 2015)	15	15
Continuous Auditing: Financial Controls – Phase 2 (October – April 2016)	15	16
Continuous Auditing: Student Data Controls – Phase 1 (August– October 2015)	15	12*
Continuous Auditing: Student Data Controls – Phase 2 (November– March 2016)	15	13*
Management Information: Data Quality	10	10
HR System Implementation	10	2**
Research and Enterprise Contracts	10	10
Risk Management	5	5
Value for Money	5	5
Prevent	0	10**
Information Security	10	10
Audit management and follow up	15	15
Total	125	123

* The scope of the Student Data Continuous Audit was reduced in 2015/16 from 30 days in total to 25 days. Our work over UKVI controls was omitted as London South Bank University procured the services of an external firm which covered this area of testing.

** The 2015/16 Internal Audit Plan initially included a ten day review on the implementation of the new HR system. This review was pushed back due to delays in the project. Two days have been included above to reflect the time already spent on this assignment. This review is included in the 2016/17 Internal Audit Plan. A review on Prevent was added to the 2015/16 plan as a replacement.

4. Follow up work conducted

Introduction

In order for the organisation to derive maximum benefit from internal audit, agreed actions should be implemented.

Within the Internal Audit Risk Assessment and Internal Audit Plan 2015/16, ten days were assigned for following up agreed actions raised in previous and current periods in order to assess whether agreed actions had been implemented by management. The table below summarises the follow up work performed.

Where findings were classified as critical, high or medium risk, we have validated that management's actions have been implemented. Where findings were classified as low risk or advisory, our follow up is limited to discussing progress with management and accepting their assurances with regards to the implementation status.

If some action has been taken to implement an action then the action has been classified as 'partially implemented'. If no action has been taken, this has been classified as 'outstanding'. We have agreed revised implementation deadlines for all 'partially implemented' actions.

Follow up work was not undertaken on findings from our Continuous Auditing programme. This is because issues noted as part of Continuous Auditing are followed up each testing period.

Summary

16 agreed actions were due for implementation in 2015/16. The table below shows that 88% of agreed actions had been fully implemented by 31 July 2016.

<i>Status</i>	<i>Number of agreed actions due by 31/07/2016</i>
Implemented	14
Partially implemented and deferred to 2016/17	2
Not implemented	0
Total	16

There are two agreed actions (12%) which were due to have been resolved by year end, but additional work is required to close the action. We agreed revised implementation deadlines for these findings and have included a breakdown of these findings, with their current status and revised implementation deadlines in Appendix 4.

We will continue to work collaboratively with management in 2016/17 to ensure that implementation timescales agreed for management actions in year are achievable, taking in to account any known or expected changes in London South Bank University's processes or regulatory requirements.

Appendices

Appendix 1: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have prepared the Internal Audit Annual Report 2015/16 and undertaken the agreed programme of work as agreed with management and the Audit Committee. Our work has been performed subject to the limitations outlined below.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound arrangements and systems for risk management, internal control and governance. Additionally, management is responsible for putting in place proper arrangements to secure economy, efficiency and effectiveness in its use of resources and to ensure proper stewardship and governance. Management is responsible for the regular review of the adequacy and effectiveness of these arrangements.

Management is responsible for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibility for the design and operation of these controls.

We 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, and our examinations as internal auditors should not be relied upon to disclose all fraud, defalcations or other irregularities which may exist.

Opinion

The opinion is based solely on the work undertaken as part of the agreed Internal Audit Risk Assessment and Internal Audit Plan 2015/16. The work addressed the control objectives agreed for each individual internal audit assignment as set out in our Internal Audit Risk Assessment and Internal Audit Plan 2015/16.

There might be weaknesses in the system of internal control that we are not aware of because they did not form part of our programme of work, were excluded from the scope of individual internal audit assignments or were not brought to our attention. As a consequence management and the Audit Committee should be aware that our opinion may have differed if our programme of work or scope for individual reviews was extended or other relevant matters were brought to our attention.

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. 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.

Future periods

Our assessment of controls relating to London South Bank University is for the year ended 31/07/2016. Historic evaluation of effectiveness may not be 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.

Appendix 2: Opinion types

The table below sets out the four types of opinion that we use, along with an indication of the types of findings that may determine the opinion given. The Head of Internal Audit will apply his/her judgement when determining the appropriate opinion so the guide given below is indicative rather than definitive.






Type of opinion	Indication of when this type of opinion may be given
Satisfactory	<ul style="list-style-type: none"> A limited number of medium risk rated weaknesses may have been identified, but generally only low risk rated weaknesses have been found in individual assignments; and None of the individual assignment reports have an overall report classification of either high or critical risk.
Generally satisfactory with some improvements required	<ul style="list-style-type: none"> Medium risk rated weaknesses identified in individual assignments that are <i>not significant in aggregate</i> to the system of internal control; and/or High risk rated weaknesses identified in individual assignments that are <i>isolated</i> to specific systems or processes; and None of the individual assignment reports have an overall classification of critical risk.
Major improvement required	<ul style="list-style-type: none"> Medium risk rated weaknesses identified in individual assignments that are <i>significant in aggregate but discrete parts</i> of the system of internal control remain unaffected; and/or High risk rated weaknesses identified in individual assignments that are <i>significant in aggregate but discrete parts</i> of the system of internal control remain unaffected; and/or Critical risk rated weaknesses identified in individual assignments that are <i>not pervasive</i> to the system of internal control; and A <i>minority</i> of the individual assignment reports may have an overall report classification of either high or critical risk.
Unsatisfactory	<ul style="list-style-type: none"> High risk rated weaknesses identified in individual assignments that <i>in aggregate are pervasive</i> to the system of internal control; and/or Critical risk rated weaknesses identified in individual assignments that are <i>pervasive</i> to the system of internal control; and/or <i>More than a minority</i> of the individual assignment reports have an overall report classification of either high or critical risk.
Disclaimer opinion	<ul style="list-style-type: none"> An opinion cannot be issued because insufficient internal audit work has been completed. This may be due to either: <ul style="list-style-type: none"> Restrictions in the audit programme agreed with the Audit Committee, which meant that our planned work would not allow us to gather sufficient evidence to conclude on the adequacy and effectiveness of governance, risk management and control; or We were unable to complete enough reviews and gather sufficient information to conclude on the adequacy and effectiveness of arrangements for governance, risk management and control.

Appendix 3: Basis of our classifications

Report classifications

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

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

<i>Finding rating</i>	<i>Points</i>
 Critical risk	40 points per finding
 High risk	10 points per finding
 Medium risk	3 points per finding
 Low risk	1 point per finding
 Advisory	0 points per finding

Individual finding ratings

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

Appendix 4: Outstanding Recommendations

Breakdown of outstanding recommendations

There are two agreed actions which have been partially implemented by 31 July 2016. We have provided a breakdown of the original finding raised, agreed action, risk rating, status and revised due date below.

Partially Implemented

Review	Agreed Action	Risk Rating	Original due date	Revised due date	Status
Change Portfolio	<p>Benefits Management</p> <p>Guidance for identifying project benefits: Alongside the implementation of the London South Bank University project management approach, a strategy and guidance for the definition, identification and specification of benefits is in development. This will support the creation and approval of business cases for investment.</p> <p>Reporting: benefits monitoring has now been built into monthly project reports, and an online reporting process is in development.</p> <p>Project closedown reports: benefits realisation: Within the 12-month project review process (noted against the previous finding), all identified benefits will be assessed to ensure they have been delivered or are on track. Guidance and oversight will ensure a consistent approach across London South Bank University projects.</p>	<p>●</p> <p>Medium</p>	30/11/2015	31/07/2016	<p>Guidance on benefits has not been completed. This shall be developed following the development of the project management methodology and business case approach which has been delayed pending recruitment of Deputy Director, Innovation & Transformation.</p> <p>The online reporting system has been implemented.</p>
Change Portfolio	<p>Portfolio Scope and Remit</p> <p>The role of portfolio management is clear – to provide oversight and support to development (or transformational) projects. Roles and accountabilities will not be developed further at this level. Activity is focussed on:</p> <ul style="list-style-type: none"> Establishing a best-in-class project management approach, detailing roles, accountabilities and controls on development projects across London South Bank University – building on the best practice approach recently introduced in ICT and existing practice across the University 	<p>●</p> <p>Medium</p>	30/11/2015 31/07/2016	31/01/2017	<p>An adapted project management methodology for business change projects is still in development. This on hold pending recruitment of Deputy Director, Innovation & Transformation.</p> <p>12-month reviews of closed projects are still planned, however none have been conducted since the Audit report was issued.</p>

	<ul style="list-style-type: none"> • Benefits approach, stakeholder engagement process, and resource management approach (detailed against relevant findings, further in this document) • Implementation of a 12-month project review process, including lessons learnt process. This is planned for projects delivered within the Change Programme, and will be detailed, with clear roles, responsibilities and outputs, in the London South Bank University project management approach. 				
--	---	--	--	--	--

Appendix 5: Mapping of internal audit work

Reporting responsibilities

The table below maps our internal audit work against the Audit Committee's reporting responsibilities.

<i>Audit Unit</i>	<i>Governance</i>	<i>Risk management</i>	<i>Control</i>	<i>Value for money</i>	<i>Data quality</i>
Continuous Auditing: Financial Controls – Phase 1 (May to July 2014)	x	x	✓	x	x
Continuous Auditing: Financial Controls – Phase 2 (October – April 2015)	x	x	✓	x	x
Continuous Auditing: Student Data Controls – Phase 1 (August– October 2014)	x	x	x	x	✓
Continuous Auditing: Student Data Controls – Phase 2 (November– March 2015)	x	x	x	x	✓
Management Information: Data Quality	x	x	x	-	✓
Research and Enterprise Contracts	x	x	x	-	✓
Risk Management	x	✓	-	-	-
Value for Money	-	-	-	✓	-
Prevent	✓	x	-	-	-
Information Security	✓	✓	x	-	x

Key

- ✓ Testing focused on this area
- x Testing was peripheral
- Not tested

Data Quality

The Audit Committee's Annual Report must include an opinion on the adequacy and effectiveness of arrangements for the management and quality assurance of data submissions to HESA, HEFCE and other funding bodies. To assist the Audit Committee prepare its Annual Report, we have outlined where our work assessed the arrangements for the management and quality assurance of data (see the table on this page). We provide no conclusions or opinion on data quality.



In the event that, pursuant to a request which London South Bank University received under the Freedom of Information Act 2000 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the “Legislation”), it is required to disclose any information contained in this terms of reference, it will notify PwC promptly and consult with PwC prior to disclosing such information. London South Bank University agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Act to such information. If, following consultation with PwC, London South Bank University discloses any such information, 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.

This document has been prepared only for London South Bank University and solely for the purpose and on the terms agreed with London South Bank University in our agreement dated 15/05/2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom), which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Internal Audit Charter 2016 – 2017
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with the Charter for the Internal Audit programme for the 16/17 Academic Year.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	The internal audit charter provides a framework for conduct of the internal audit activity within the plan for 16/17 & the assurance this provides for the controls and processes that relate to the entire organisation.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the charter

Matter previously considered by:		
Further approval required?		

Executive Summary

The Internal Audit Charter sets out the framework within which the internal audit activity is conducted at LSBU.

It clarifies the purpose and scope of the activity, and outlines the authority, responsibility and independence of the process

The Charter is accompanied by the Internal Audit Plan in Final Version. This was approved at the June Audit Committee meeting.

- The Committee is requested to approve the charter & note the Internal Audit Plan in Final.

Internal Audit Charter

*London South Bank
University*

*Draft
September 2016*

Page 200

Distribution List:

Audit Committee Members

Richard Flatman – Chief Financial Officer

**James Stevenson – University Secretary to the Clerk of the
Board of Governors**

Purpose and scope



This Internal Audit Charter provides the framework for the conduct of the Internal Audit function in London South Bank University (LSBU) and has been approved by the Audit Committee. It has been created with the objective of formally establishing the purpose, authority and responsibilities of the Internal Audit function.

Purpose

Internal Auditing is an independent, objective assurance and consulting activity designed to add value to and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

Scope

All of LSBU's activities (including outsourced activities) and legal entities are within the scope of Internal Audit. Internal Audit determines what areas within its scope should be included within the annual audit plan by adopting an independent risk based approach. Internal Audit does not necessarily cover all potential scope areas every year. The audit program includes obtaining an understanding of the processes and systems under audit, evaluating their adequacy, and testing the operating effectiveness of key controls. Internal Audit can also, where appropriate, undertake special investigations and consulting engagements at the request of the Audit Committee, senior management and regulators.

Internal Audit will coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts.

Authority, responsibility and independence



Authority

The Internal Audit function of LSBU derives its authority from the Board through the Audit Committee. The Head of Internal Audit is authorised by the Audit Committee to have full and complete access to any of the organisation's records, properties and personnel. The Head of Internal Audit is also authorised to designate members of the audit staff to have such full and complete access in the discharging of their responsibilities, and may engage experts to perform certain engagements which will be communicated to management. Internal Audit will ensure confidentiality is maintained over all information and records obtained in the course of carrying out audit activities.

Responsibility

The Head of Internal Audit is responsible for preparing the annual audit plan in consultation with the Audit Committee and senior management, submitting the audit plan, internal audit budget, and resource plan for review and approval by the Audit Committee, implementing the approved audit plan, and issuing periodic audit reports on a timely basis to the Audit Committee and senior management.

The Head of Internal Audit is responsible for ensuring that the Internal Audit function has the skills and experience commensurate with the risks of the organisation. The Audit Committee should make appropriate inquiries of management and the Head of Internal Audit to determine whether there are any inappropriate scope or resource limitations.

It is the responsibility of management to identify, understand and manage risks effectively, including taking appropriate and timely action in response to audit findings. It is also management's responsibility to maintain a sound system of internal control and improvement of the same. The existence of an Internal Audit function, therefore, does not in any way relieve them of this responsibility. Management is responsible for fraud prevention and detection. As Internal Audit performs its work programs, it will be observant of manifestations of the existence of fraud and weaknesses in internal control which would permit fraud to occur or would impede its detection.

Independence

Internal Audit staff will remain independent of the business and they shall report to the Head of Internal Audit who, in turn, shall report functionally to the Audit Committee and administratively to the Chief Financial Officer.

Internal Audit staff shall have no direct operational responsibility or authority over any of the activities they review. Therefore, they shall not develop nor install systems or procedures, prepare records or engage in any other activity which they would normally audit. Internal Audit staff with real or perceived conflicts of interest must inform the Head of Internal Audit, then the Audit Committee, as soon as these issues become apparent so that appropriate safeguards can be put in place.

Professional competence, reporting and monitoring



Professional competence and due care

The Internal Audit function will perform its duties with professional competence and due care. Internal Audit will adhere to the Definition of Internal Auditing, Code of Ethics and the Standards for the Professional Practice of Internal Auditing that are published by the Institute of Internal Auditors.

Reporting and monitoring

At the end of each audit, the Head of Internal Audit or designee will prepare a written report and distribute it as appropriate. Internal Audit will be responsible for appropriate follow-up of audit findings and recommendations. All significant findings will remain in an open issues file until cleared by the Head of Internal Audit or the Audit Committee.

The Audit Committee will be updated regularly on the work of Internal Audit through periodic and annual reports. The Head of Internal Audit shall prepare reports of audit activities with significant findings along with any relevant recommendations and provide periodic information on the status of the annual audit plan.

Periodically, the Head of Internal Audit will meet with the Chair of the Audit Committee in private to discuss internal audit matters. The performance of Internal Audit will be reported periodically to Senior Management and the Audit Committee.

Definitions



Board of Governors

The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organisation.

Throughout this document, the term ‘Board’ refers to the Board of Governors.

University Executive

The University Executive is responsible for the executive management of LSBU and its day-to-day direction in accordance with the priorities set by the Board.

Throughout this document, the term ‘Executive’ refers to the University Executive.

Audit Committee

The governance group charged with independent assurance of the adequacy of the risk management framework, the internal control environment and the integrity of financial reporting.

Senior Management

The individuals at the highest level of organisational management who have day-to-day responsibility for managing the organisation.

Head of Internal Audit

Head of Internal Audit describes a person in a senior position responsible for effectively managing the internal audit activity.

This role is fulfilled by Justin Martin, PwC Partner.

PwC Internal Audit Team



Justin Martin, Head of Internal Audit



Key contact for the Chief Financial officer and the Chair of the Audit Committee.

Co-ordinate and oversee delivery of all services and activities under the contract for LSBU – proactively build relationship with management and stakeholders.

Setting our annual programme of work, for approval by the Chief Financial Officer and Audit Committee. Attend Audit Committee, including delivery of the annual Internal Audit opinion.

Strategic deployment of PwC resources to meet LSBU’s needs. Performance of senior team members and quality review all final draft/final reports. Drive innovation and consistency.

Charlotte Bilsland, Engagement Senior Manager



Key contact for the Chief Financial Officer and the Chair of the Audit Committee.

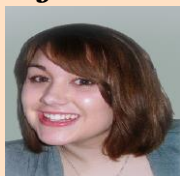
Project manage overall engagement delivery and team members’ performance.

Engage with key stakeholders and the audit team to bring insight on technical issues, sector development and share benchmarked information.

Any issues for escalation can also be reported to Charlotte independently.

Quality assurance of fieldwork and deliverables.

Lucy Gresswell, Engagement Manager



Key contact for the Chief Financial Officer and the Chair of Audit Committee.

Project manage delivery of agreed audit assignments including team members’ performance, scoping terms of reference for audits and review/quality assurance of project fieldwork performed by team.

Brief team members about LSBU and issues relevant to specific projects

Co-ordinate activities and delivery of the team to ensure value for money is achieved.

In the event that, pursuant to a request which LSBU has received under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004 (as the same may be amended or re-enacted from time to time) or any subordinate legislation made thereunder (collectively, the "Legislation"), LSBU is required to disclose any information contained in this document, it will notify PwC promptly and will consult with PwC prior to disclosing such document. LSBU agrees to pay due regard to any representations which PwC may make in connection with such disclosure and to apply any relevant exemptions which may exist under the Legislation to such [report]. If, following consultation with PwC, LSBU discloses any this document 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.

This document has been prepared only for LSBU and solely for the purpose and on the terms agreed with LSBU in our agreement dated 15 May 2015. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

	CONFIDENTIAL	
Board/Committee:	Audit Committee	
Date:	22 September 2016	
Paper title:	Pension assumptions at 31/7/16	
Author:	Natalie Ferer – Financial Controller	
Executive sponsor:	Richard Flatman – Chief Financial Officer	
Recommendation by the Executive:	The Executive recommend that the committee approves the assumptions made by the LPFA scheme actuaries, Barnet Waddington, and the assumptions used for the USS scheme for accounting disclosures.	
Aspect of the Corporate Plan to which this will help deliver?	Statutory financial reporting.	
Matter previously considered by:	Audit Committee	Annually
Further approval required?	n/a	n/a
Communications – who should be made aware of the decision?	N/A	

Executive summary

This paper is being presented to Committee because the assumptions used by the actuaries in respect of the LGPS have a significant impact on our reported financial result including the reported scheme deficit. It is important therefore that the assumptions are reviewed and approved.

Indicative assumptions for the LSBU report at 31/7/16 have already been circulated to members of committee. The final assumptions have now been received and are set out herein.

We have taken advice from Grant Thornton, the University's auditors, and are recommending the standard assumptions shown which Grant Thornton have confirmed are in line with the benchmark across the sector.

The assumptions are have changed significantly from the indicative assumptions circulated to audit committee members in June and have resulted in a net deficit in the scheme of **£121.5m with £38.3m being charged to the statement of consolidated income and expenditure**. Full details of the resulting pension deficit and charge to the accounts will be presented in the financial statements and auditors report later in the year.

Assumptions

The report for London South Bank University has been prepared using standard scheme assumptions which are summarised below:

	31/7/16 Final	31/7/16 Indicative	31/7/15	31/7/14
RPI increases	3.0%	3.3% - 3.1%	3.5%	3.5%
CPI increases	2.1%	2.4% - 2.2%	2.6%	2.7%
Salary increases	3.9%	4.2% - 4.0%	4.4%	4.6%
Pension increases	2.1%	2.4% - 2.2%	2.6%	2.7%
Discount rate	2.5%	3.4%- 3.1%	3.8%	4.2%

More detailed analysis of the assumptions are contained in Appendix 1.

The most significant variation in assumption compared to the indicative assumption is in the discount rate which has fallen from 3.8% at 31/7/15 to 2.5% at 31/7/16. As detailed in appendix 1, most employers, including LSBU have seen a substantial decrease in funding levels this year. This is primarily due to the fall in corporate bond yields over the last few months, particularly in the period following the EU referendum, which has driven down the discount rates and in turn significantly increased the deficit in the scheme. The deficit for LSBU has risen from £88.7 as at 31/7/15 to £121.5m as at 31/7/16. The real discount rate, which ultimately raises the level of deficit, is the net of the underlying discount rate and CPI and is now at a very low level of 0.4% (31/7/15 1.2% and 31/7/14 1.5%).

USS scheme

For the first time, in line with FRS102, the University is required to account for its share of assets and liabilities in the USS pension scheme on its balance sheet. To do this the University has calculated its share of the deficit in the USS scheme using a model published by the British University's Finance Directors Group (BUFDG) and the University must chose the assumptions it uses when making this calculation. Our

auditors have previously indicated that it is reasonable for us to use the same discount rate and salary increase assumptions for the USS scheme as we do for the LPFA scheme. This calculation results in a deficit in the University's share of the USS scheme of **£1.0m with £528k being charged to the consolidated statement of income and expenditure.**

Recommendation

The Committee is asked to note and approve the assumptions.

Subject FRS102 and IAS19 final assumptions for 31 July 2016

Background

We have been asked to provide the assumptions that will be adopted for the FRS102/IAS19 disclosures at 31 July 2016.

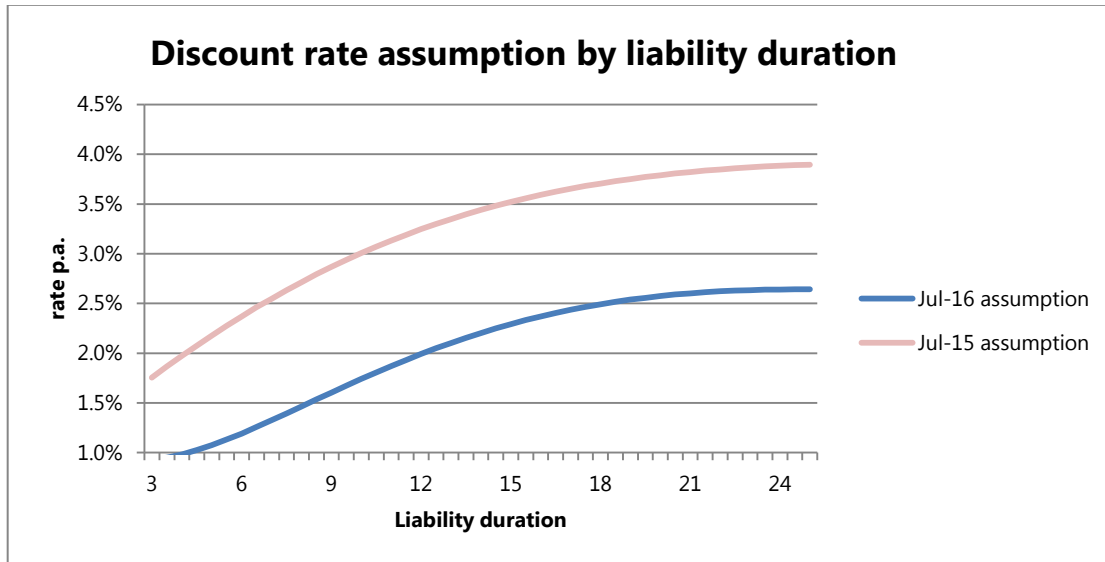
This note discusses our recommended assumptions for the exercise, however the responsibility for setting assumptions ultimately belongs to the employer and therefore if an employer was to request alternative assumptions then we would be happy to use these in producing our report for the employer. **The assumptions in this report are therefore the standards that we would intend to use, should we not be instructed otherwise.** We believe that these assumptions are likely to be appropriate for most employers but we have not consulted with each employer in setting these.

Employers that previously accounted under FRS17 will now account under FRS102. For these employers, we will produce full comparator figures under FRS102 for the period to 31 July 2015 alongside last year's disclosed FRS17 figures. At the end of this note we also include key details of the new FRS102 standard.

Discount rate

Our standard approach for the July 2016 exercise will be to use the point on the annualised Merrill Lynch AA rated corporate bond yield curve based on the estimated duration of each employer's liabilities. For employers with an estimated duration of greater than 25 years, we will use the 25 year point on the curve. This is the same approach as last year.

The following graph shows the assumption by liability duration at 31 July 2016, together with the standard assumption at 31 July 2016.



Our reports will disclose our estimate of each employer's liability duration.

As bond yields have fallen very sharply over the last few months, the discount rate yield curve is currently around 1.0-1.3% p.a. lower than at 31 July 2015, depending on the point on the curve.

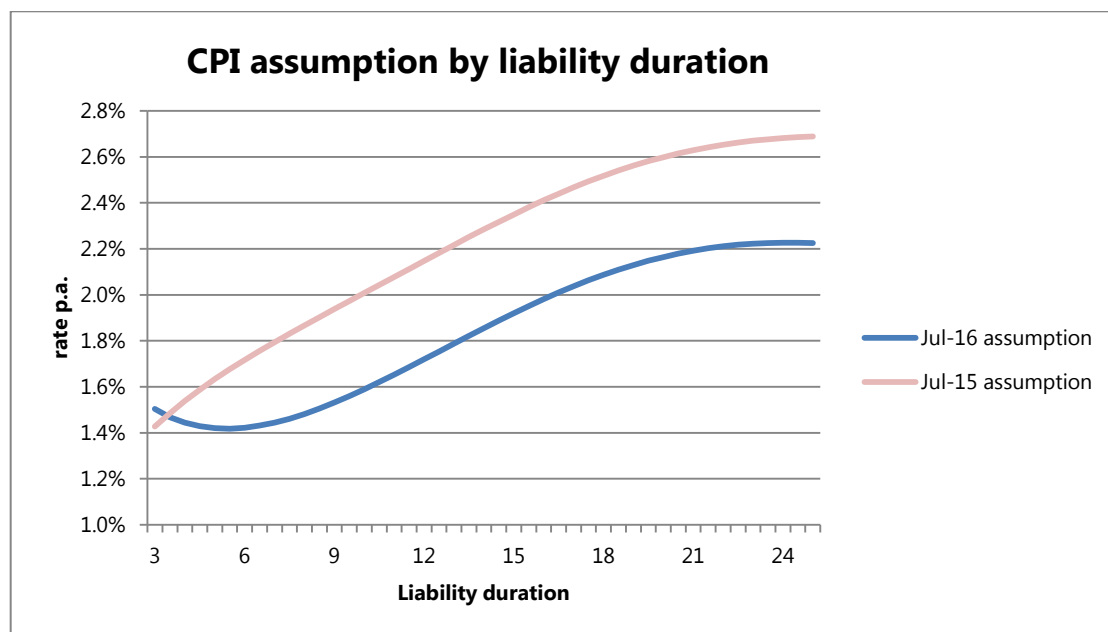
Inflation and salary increases

Our standard approach will be to take the rate at each employer's duration implied by the Bank of England's future Retail Prices Index (RPI) inflation curve which is based on the difference in conventional and index-linked gilt yields. This is the same approach as was taken for the July 2015 exercise.

The indexation of pensions in the public sector is expected to be in line with the Consumer Prices Index (CPI). Unlike RPI, there are very few traded CPI instruments and so a price cannot be directly observed in the market. We therefore base our CPI assumption on the assumption we make for RPI.

CPI has historically been below RPI and so we are likely to assume that it will, on average, be 0.9% per annum less than RPI. We believe that this is a reasonable estimate for the future differences in the indices, based on the different calculation methods.

The following graph shows our assumptions for CPI inflation by liability duration at 31 July 2016.



At medium to long terms, inflation is 0.4-0.5% p.a. lower than at 31 July 2015 (although the gap reduces at shorter terms).

Our starting point for the salary increase assumption will be that made for the 2013 triennial valuation, i.e. the salary increase assumption will be 1.8% per annum above CPI. This is the same as the approach adopted last year.

Mortality

The mortality assumption we have adopted for this year's accounting disclosures will be the mortality assumptions provided by Club Vita in line with those disclosed in the 2013 funding valuation for the LPFA Pension Fund. We have also made an allowance for future improvement factors in line with the 2012 CMI model with a long term assumption of 1.5% p.a. This is the same as the approach adopted last year.

Club Vita analyse mortality on an individual level and so the mortality assumptions should better reflect employer membership structure than a single assumption for the Fund.

Combined effect on liabilities

The table below describes the likely effects for employers at 5 year duration points, based on market conditions at 31 July 2016.

Term	Effect of changes in financial assumptions on employer's liabilities using market conditions as at 31 July 2016
5 years	Approx. 5% increase in liabilities
10 years	5-10% increase in liabilities
15 years	10-15% increase in liabilities
20 years	15-20% increase in liabilities
25 years	Approx. 20% increase in liabilities

Assets and overall deficit

We have data for the LPFA's asset returns for the period to 31 May 2016. These show flat returns for the 10 month period (allowing for estimations made at the July 2015 exercise).

Since then both equity and gilt markets have risen significantly so we estimate that the return for the period might be around 5%. Based on this figure, we'd expect a small positive effect from asset performance for all employers.

Overall, based on current market conditions, we believe that most employers will see substantial decrease in funding levels this year. This is primarily due to the fall in corporate bond yields over the last few months, particularly in the period following the EU referendum, which has driven down the discount rates and in turn increased the defined benefit obligation significantly, as shown above.

New FRS102 standard

The new FRS102 standard applies to employers who have an accounting year beginning on or after 1 January 2015 although earlier adoption was permitted.

The key changes under the new FRS102 standard are as follows:

- The “expected return on assets” figure will no longer be used. Instead, the “finance cost” which is currently the difference between the interest on liabilities and expected return on assets will be replaced by a “net interest cost”, calculated using the discount rate applying at the start of the period;
- Discount rates are no longer specifically pegged to AA-rated bonds, only to “high quality corporate bonds”, although it is not expected that this change will have much of an impact.
- More disclosures will be required about the risks posed by the fund;
- Various components within the disclosures will be relabelled;
- More detailed disclosure about the fund assets;
- The cost of a defined benefit scheme will be divided into four elements, the first three of which will be included in profit/loss, the fourth in other comprehensive income:
 1. Change in liability due to employee service during the reporting period (service cost)
 2. Net interest on the net liability
 3. Benefit changes, curtailments and settlements (past service costs)
 4. Re-measurement of the liability (comprising actuarial gains and losses and the return on the fund assets (excluding the net interest amount))
- FRS 102 refers to the “fair value” of assets rather than specifically requiring the use of bid values;
- Treatment of expenses - administration costs, other than those relating to investment management, will need to be expensed as they are incurred.

The introduction of FRS102 may also affect how employers disclose their liabilities from unfunded schemes. If employers participate in unfunded multi-employer schemes such as the Teachers' Pension Scheme or the NHS Pension Scheme, the nature of these schemes means that they will probably account for them as if it was a defined contribution scheme (i.e. the pension costs are simply the contributions paid) even though they are defined benefit schemes. For these schemes, employers will need to recognise on their balance sheet the expected present value of all future deficit reduction contributions.

If you have any questions please contact your usual team member.

Barnett Waddingham LLP

02 August 2016

This page is intentionally left blank

	CONFIDENTIAL
Board/Committee	Audit Committee
Date of meeting:	7 th September 2016
Paper title:	External Audit Sourcing Strategy
Author:	Robert Ager
Sponsor:	Richard Flatman
Purpose:	To ensure that adequate audit arrangements are in place.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This will support the Corporate Objectives covered by Resources and Infrastructure, particularly related to financial controls.
Recommendation:	Re-tender via option 3 – Crown Commercial Service Consultancy ONE framework.
Matter previously considered by:	Executive
Further approval required?	Final approval required by the Audit Committee

Executive Summary

This strategy document is for the re-tender of the External Audit Services contract. The strategy is to determine how key issues will be addressed – such as route(s) to market, stakeholders, timescale and evaluation criteria – and translated into the procurement process and documentation. It identifies and minimises risk and assists in ensuring all key factors have been taken into account when conducting the procurement, leading to fit for purpose contracts offering value for money.

London South Bank University

Procurement Services – Sourcing Strategy

Tender Title: External Audit Services

Reference: 16-002

This strategy document is for the re-tender of the External Audit Services contract. The strategy is to determine how key issues will be addressed – such as route(s) to market, value analysis, stakeholders, timescale and evaluation criteria – and translated into the procurement process and documentation. It identifies and minimises risk and assists in ensuring all key factors have been taken into account when conducting the procurement, leading to fit for purpose contracts offering value for money.

1. Background Information

Category	Professional Services/Finance
Description of Tender	<p>The University's current External Audit services contract (with Grant Thornton) ends on 31 July 2017. The University is seeking a provider of external audit services who can offer a distinctive, innovative, proactive and professional approach to external audit, and one that meets all the external audit requirements in the HEFCE Audit Code of Practice.</p> <p>The service provider will:</p> <ul style="list-style-type: none"> ○ conduct the audit of London South Bank University and companies that are wholly-owned subsidiaries of the University, which at August 2016 were: South Bank University Enterprises (SBUEL) ○ be required to provide a service that as a minimum covers the Accounts Directions or applicable Codes of Practice issued by the Higher Education Funding Council for England (HEFCE), the Charity Commission's Statement of Recommended Practice on Accounting and Reporting by Charities (SORP), and all applicable Accounting standards. ○ provide assurance to the University's Board and Audit Committee on the University's governance and internal control system, including risk management.
Procurement Lead	Rob Ager
New or repeat tender	Repeat

London South Bank University

EU or Non EU If EU compliant, is a collaborative route available?	EU compliant
Estimated contract value per year	£60,000
Estimated contract value of entire contract life (including possible extensions)	£420,000
Proposed Contract duration	5 years with the option to extend by a further 2x1 years

2. Stakeholders

<p>Working Group Members and key stakeholders.</p> <p>Richard Flatman – Chief Financial Officer Natalie Ferer – Financial Controller Audit Committee GovLegal</p>
--

3. Business Need

<p>It is a legal and regulatory requirement to appoint external auditors to audit London South Bank University and its subsidiaries. The external auditors will be responsible for performing the audit and expressing opinions on the financial statements.</p>
--

4. Routes to Market

<p>Option 1 – Open tender advertised via OJEU</p> <p>Tendering process likely to take around 4 months to complete. Any company wishing to submit a bid can do so and LSBU is required to assess all compliant bids.</p> <p>Option 2 – Mini-Competition from APUC Audit Services Framework.</p> <p>Reduced tendering time and capped day rates for all levels of seniority. Pre-defined Terms and Conditions and mitigation from any EU risk. Only suppliers on the framework can be invited. Previous use of this framework by other London & SE institutions has led to the suggestion that some companies do not wish to work outside of Scotland and the north.</p> <p>Option 3 – Mini-Competition from the Crown Commercial Service (CCS) Consultancy ONE Framework.</p> <p>Reduced tendering time and capped day rates for all levels of seniority. Pre-defined Terms and Conditions and mitigation from any EU risk. Only suppliers on the framework can be invited.</p>

London South Bank University

<p>Suppliers on APUC Framework (option 2)</p> <p>KPMG Ernst & Young Grant Thornton French Duncan Wylie & Bassett Henderson Loggie Mazars Scott Moncrieff</p>	<p>Suppliers on CCS Framework (option 3)</p> <p>KPMG Ernst & Young Grant Thornton BDO Deloitte Moore Stephens PwC RSM Tax & Accounting</p>
<p>The BUFDG audit survey details the audit firms that 117 Universities used for the audit of their 2014/15 Financial Statements. The Survey had a 67% response rate and shows that 95% of the 117 respondents use one of the 6 audit firms listed below. These 6 firms also cover 100% of the Universities covered with turnover of between £100m and £200m.</p>	
<p>KPMG Deloitte PWC Grant Thornton BDO Ernst and Young</p>	
<p>The remaining 5% are covered by firms that for 2014/15 only audited respondent Universities with turnover of less than £20m.</p>	
<p>Mazars Buzzacott Chiene and Tait</p>	
<p>Option 2 lists 3 of the 6 firms but excludes Deloitte, PWC and BDO. Option 3 includes all 6. The recommendation is option 3 as it is unlikely that the University would receive a credible tender from a firm not already on the option 3 list if we opted for an open tender.</p>	
<p>The previous tendering process held in 2010 was a competitive process conducted in accordance with the open procedure under the Public Contracts Regulations 2006. Bids were received from:</p> <p>BDO Deloitte Grant Thornton Cansdales</p>	

5. Evaluation Criteria & Weightings

To be agreed if open market route is selected. Otherwise, framework headline criteria will apply.

Criteria	Weighting
Quality – to be determined by tender panel	60% - 80%
Price – to be determined by tender panel	40% - 20%

6. Ethical Procurement

Standard Employability text and questions to be included in the tender
--

7. Estimated Savings and Cost Variances

Savings against the current contract are not anticipated due to the nature of the required services.
--

8. Anticipated Timeline

Key Stage	Planned date for completion
Sourcing Strategy approval – stage 1	Executive 7 th September
Sourcing Strategy approval – stage 2	Audit Committee 22 nd September
OJEU Notice Advertised	
PQQ Issued	
PQQ Returned	
PQQ Evaluation and Shortlist	
ITT Issued	
ITT Return Date	
ITT Evaluation	
10 Day standstill period ends	
Award Contract	Estimated end of March 2017
Other (please specify)	

9. Procurement Risk Register

Key Risk to be Considered	Likelihood (Low, Medium, High)	Impact (Low, Medium, High)	Mitigation Action

10. Submission and approval

Submitted by Lead Stakeholder:	
Date:	

Approved by Procurement:	
Date:	

Approved by Head of Procurement:	
Date:	

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Corporate Risk Register
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	John Baker – Corporate & Business Planning Manager
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with the current corporate risk register.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	All aspects as the risk entries on the register are aligned to the goals of the Corporate Strategy.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the risks and their ratings, • the allocation of risks to corporate objectives

Matter previously considered by:	Strategic Risk Review Group	On: 6 th September
Further approval required?		

Executive Summary

The latest version of the Corporate Risk Register is attached for review.

The Strategic Risk Review Group met in September, and reviewed the entries on the register. This updated version of the register incorporates changes agreed at that meeting, with an overview of the key amendments provided in the middle column of the summary table on pages 2 and 3.

The Committee is requested to note:

- the risks and their ratings
- the allocation of risks to corporate objectives

LSBU Corporate Risk Register cover sheet: Risk overview matrix by impact & residual likelihood

Date: 12thth Sep 2016

Author: John Baker – Corporate & Business Planning Manager

Executive Lead: Richard Flatman – Chief Financial Officer

	<p>2: Revenue reduction if marketing and PR activity does not achieve H/EU UG recruitment targets (IM)</p>	<p>1: Lack of capability to respond to policy changes & shifts in competitive landscape (DP)</p>	<p>4 Critical <i>fail to deliver corporate plan / removal of funding or degree awarding status, penalty / closure</i></p>	Impact
<p>157: Anticipated international student revenue unrealised (PI)</p>	<p>6: Management Information perceived as unreliable, doesn't triangulate or is not presented (RF) 14: Loss of NHS contract income (WT) 305: Data not used / maintained securely (IM) 362: Low staff engagement impacts performance negatively (DP) 3: Increasing pensions deficit reduces flexibility (RF) 402: Unrealised research & enterprise £ growth (PI) 467: Progression rates don't rise (PB) 495: Higher Apprenticeship degrees (PB)</p>	<p>37: Affordability of Capital Expenditure investment plans (RF)</p>	<p>3 High <i>significant effect on the ability for the University to meet its objectives and may result in the failure to achieve one or more corporate objectives</i></p>	
<p>517: Impact of EU Referendum result on operating conditions & market trends (DP)</p>	<p>398: Academic programmes not engaged with technological and pedagogic developments (SW)</p>	<p>494: Inconsistent delivery of Placement activity across the institution (SW)</p>	<p>2 Medium <i>failure to meet operational objectives of the University</i></p>	
			<p>1 Low <i>little effect on operational objectives</i></p>	
<p>3 - High <i>The risk is likely to occur short term</i></p>	<p>2 - Medium <i>This risk may occur in the medium term.</i></p>	<p>1 - Low <i>This risk is only likely in the long term</i></p>		
Residual Likelihood				
<p>Executive Risk Spread: VC – 2, DVC – 2, CFO – 3, PVC-S&E – 2, PVC-R&EE – 2, COO – 2, Dean Health – 1, ExD-HR – 1, US - 0</p>				

Page 224

Changes since presentation at previous AC / Operations Board meeting, and overdue action progress updates detailed below:

Reference	Risk title	Completed Actions & Risk Changes	Overdue Actions
Goal 1: Employability: Ensuring students develop skills, aspiration and confidence.			
494 (SW)	Inconsistent delivery of Placement activity across institution	<p>Appointment action implemented: Sukaina Jeraj has been seconded to the Head of Placements role from the 1st June for 6 months.</p> <p>Delivery of inPlace IT solution implemented: The live environment is now up and running in the cloud, and the Adult, Child & Mental Health nursing & Midwifery courses in HSC will be using the tool from Semester 1 16/17.</p>	
Goal 3: Teaching & Learning: Ensuring teaching is highly applied, professionally accredited & linked to research & enterprise			
398 (SW)	Low engagement with tech or pedagogic developments	<p>Pilots & subject interventions completed: The investments from the teaching and learning fund were utilised for this activity. The embedding of study skills within modules has already seen improvements in pass rates and progression.</p> <p>New Actions added – Team & User group</p>	
467 (PB)	UG Progression rate doesn't rise	<p>Learner Analytics Plan action implemented: The Learner Analytics Plan has been developed. ICT clarifying timescales for the next stages.</p> <p>New Actions added – new interns, strategy review, Analytics rollout & amendments to regulations.</p>	
Goal 4: Research & Enterprise: Delivering outstanding economic, social and cultural benefits from our intellectual capital.			
402 (PI)	2020 income growth through Research & Enterprise	<p>Pipeline report action implemented. The new Ops Board report draws information directly from Raiser's Edge and Agresso.</p> <p>New Actions added – bid management and guide launch.</p>	
Goal 5: Access: Work with local partners to recruit, engage and retain students with the potential to succeed.			
495 (PB)	Impact of Higher Apprenticeship degrees on existing recruitment markets	<p>Action to develop plan implemented: This action was completed, with Alison May appointed and Hefce funds acquired for the 16/17 year.</p> <p>New action added – Team recruitment.</p>	
Goal 6: Internationalisation: Developing a multicultural community of students & staff through alliances & partnerships.			

457 (PI)	International student £income unrealised		
517 (DP)	Impact of EU Referendum	New Risk Entry	
Goal 7: People & Organisation: Attracting proud, responsible staff, & valuing & rewarding their achievements.			
1 (DP)	Response to environmental change & reputation	Controls Updated. New actions: Office of Corporate Affairs, and submission of narrative TEF elements.	
362 (DP)	Poor Staff Engagement	EES actions plan strategy developed The plan was presented to June Operations Board New actions around intranet soft launch, and Progress review of actions plans, and pulse check.	
Goal 8: Infrastructure: Investing in first class facilities and outcome focused services, responsive to academic needs.			
2 (PI)	Home & EU Recruitment income targets	Previous actions implemented The strategy for 16/17 developed, along with CMA training for ambassadors, and new procedures for approval of school marketing materials. New action around scenario modelling.	
6 (RF)	Pensions deficit	Controls updated.	
6 (RF)	Quality and availability of Management Information	Phase 2 MIO Plan action completed: The FMI priority areas have been articulated to the Project Board and development is under way by the BI team within ICT. New Action added – Enrolments visualisation	
14 (WT)	Loss of NHS income	New Actions created	
37 (RF)	Estates strategy £ impact	Controls updated.	Student Centre negotiations action progress update: Programming expert engaged to adjudicate on the decisions taken in respect of the refused extension of time claim. We await a meeting with the senior Director of Balfour Beatty early in 2016.
305 (IM)	Data Security		Mandatory training action progress update: The Pilot programme completed in January, feedback from this was implemented in February and ICT are now in discussions with HR comms team to work out optimum distribution method and comms package.

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
494	Inconsistent delivery of Placement activity across institution	Shan Wareing	<p>Cause:</p> <p>Lack of allocation of sufficient central and School human resource</p> <p>insufficient expertise within LSBU</p> <p>Speed of implementation without adequate project planning or learning from the sector</p> <p>Lack of assurance over offsite workplace conditions</p> <p>Effect:</p> <p>Placement practice may not comply with Chapter B10 of the Quality Code</p> <p>All students who expect one may not be able to gain a placement, leading to a CMA risk</p> <p>Placements may not deliver a good student experience</p> <p>Duty of Care to students re workplace safety might not be met.</p> <p>Potential un-insured risk exposure</p>	<p>I = 3 L = 2 High (6)</p> <p style="background-color: red; color: black; text-align: center;">High</p>	Utilisation of InPlace management platform to ensure consistency of process and knowledge exchange.	<p>I = 3 L = 1 Medium (3)</p> <p style="background-color: yellow; color: black; text-align: center;">Medium</p>	Valerie Tomlinson	Creation of placements policy and placement agreement pro-forma.	30 Sep 2016
							John Baker	Oversee completion of Internal Audit Review into activity.	28 Feb 2017
							Valerie Tomlinson	Develop procedure and systems for quality assurance of placement opportunities.	23 Dec 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
398	Academic programmes do not employ suitable technological and pedagogic developments to support students and promote achievement	Shan Wareing	<p>Cause</p> <p>Sustained underinvestment in expertise and dedicated human resource to support utilisation of learning technologies, comparative to new and existing competitors</p> <p>Effect:</p> <p>LSBU does not effectively exploit the learning potential of new technologies, impacting negatively on student retention, achievement, or cost base (eg in terms of physical estate, inability to use virtual facilities) and our ability to delivery new provision such as apprenticeships</p> <p>Curriculum do not adapt sufficiently to remain relevant, jeopardising the employability of LSBU graduates.</p> <p>More flexible and efficient educational models which enable us to remain adaptable and competitive are out of institutional reach</p> <p>Support mechanisms do not provide some students with the learning support they need to navigate and succeed in the learning environment so retention does not meet the targets within the 5 year forecast.</p> <p>Market appeal of courses is impaired, impacting negatively on recruitment</p>	I = 3 L = 2 High (6)	Delivery of the Technologically Enhanced Learning Strategy (TEL) through the Learning Pathway Programme.	I = 3 L = 2 High (6)	Shan Wareing Marc Griffith	<p>Establish Digitally Enhanced Learning User Group - to engage with stakeholders, prioritise resources and report progress to Academic board on ongoing basis.</p> <p>Appoint to positions within DEL team to oversee MyLSBU environment and Digital Literacies projects.</p>	30 Nov 2016 23 Dec 2016



Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
467	Progression rate across undergraduate programmes does not rise in line with targets of Corporate Strategy	Pat Bailey	<p>Cause:</p> <p>Low tariff students admitted through clearing. ESE analytics dashboards not utilised. High risk students are not identified in a timely way and supported sufficiently. Students don't engage with new initiatives. Support provided fails to bridge support gap for students entering through non-traditional access routes.</p> <p>Effect:</p> <p>Progression rate fails to increase. Hefce, or OfStud, could view institution as high risk. Data could have negative impact in TEF metric assessment. Considerable lost income to institution from Y2 & Y3 potential enrolments.</p>	I = 3 L = 2 High (6)	Study Support & Skills Sessions provided by the Library &LRC	I = 3 L = 2 High (6)	Jamie Jones	Recruit 8 interns to new trial positions to create a team to help identify and support students who appear to be disengaging from their studies.	30 Sep 2016
				[REDACTED]	Student Welfare advice and support provided by Student Life Centre	[REDACTED]	Jamie Jones	Amend Academic Regulations to provide greater support to students at risk of withdrawal.	31 Mar 2017
				[REDACTED]	[REDACTED]	[REDACTED]	Jamie Jones	Review impact of Engagement and Attendance Monitoring Strategy.	31 Jul 2017
				[REDACTED]	[REDACTED]	[REDACTED]	Lesley Roberts	Oversee rollout of stage 1 of Learner Analytics Project with demographic data dashboard available to Personal Tutors and Student support teams.	31 Oct 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
402	Income growth expected from greater research and enterprise activity does not materialise	Paul Ivey	<p>Cause:</p> <ol style="list-style-type: none"> 1) Challenging market environment with high competition for similar opportunities and funders. 2) Lack of proven forecasting systems & recent static performance 3) Aggressive and complex turnaround required carries intrinsic high risk. 4) Dependence on HSC CPPD income (circa 50% of enterprise£) 5) New structures fail to entice and encourage academic participation in activity. 6) Limitations of academic capacity and capability. 7) Internal competition for staff time over and above teaching. 8) TNE partnerships are not approved, or break down when contacts relocate. <p>Effect:</p> <ol style="list-style-type: none"> 1) Income growth expectations unrealised. 2) Undiversified enterprise portfolio. 3) Lower financial contribution, as an increased proportion of delivery is sourced outside core academic staff. 4) Increased dependency on generating enterprise opportunities via Knowledge Transfer outreach as opposed to an academic-led stream, results in higher opex costs. 5) The holistic benefits for teaching and the student experience are reduced. 6) Proportion of staff resource diverted to winning new funding is significantly increased. 7) Reduced research income adversely affects the research environment, publication rates, evidence of impact, student completions, & ultimately LSBU REF 2020 rating. 8) Inability to align academic resource with identified market opportunities. 9) TNE.. 	<p>I = 3 L = 2 High (6)</p> 	<p>Operation of Sharepoint Enterprise Approval Process for authorisation of new income opportunities.</p>	<p>I = 3 L = 1 Medium (3)</p> 	<p>Onyemaechi Imonioro</p>	<p>Launch new LSBU Research & Enterprise guide to income generation.</p>	<p>30 Sep 2016</p>
					<p>R&E activity Pipeline Reports (Financial & Narrative) will be provided to each Operations Board Meeting to aid constant scrutiny and review of progress against 5 year income targets.</p>		<p>Graeme Maidment</p>	<p>Development of bid management strategy for each School.</p>	<p>22 Dec 2016</p>
					<p>Bid writing workshops for academic staff delivered routinely</p>		<p>Yvonne Mavin</p>	<p>Launch new corporate process for post award contract management; for research and enterprise contract activity.</p>	<p>30 Sep 2016</p>
					<p>Enterprise Business Plan & strategy submitted for approval annually to SBUEL Board (which has 2 Non-Executive Directors) for monitoring & quarterly updates provided at LSBU Board meetings.</p>				


Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
495	Impact of Higher Apprenticeship degrees on existing recruitment markets	Pat Bailey	Cause: Introduction of Higher Apprenticeship degrees.	I = 3 L = 2 High (6)			Pat Bailey	Develop a financial model for the efficient running of Higher and Degree Apprenticeships , with funding mechanisms for student transfer from FE-HE.	28 Oct 2016
			Opportunity: These degrees present may present an opportunity for LSBU to grow student numbers in a new market.				Alison May	Appoint staff to the new team roles being created to manage this activity for the institution.	01 Nov 2016
			Effect: These degrees could cannibalise existing employer sponsored students. This represents a risk to existing income and markets. LSBU currently has c.4,000 students on part-time courses, majority employer-sponsored & initial estimations are that income from 1,400 students (£3.3m of surplus) could be affected.				Pat Bailey	Develop launch strategy for Institute of Professional & Technical Education (IPTE)	30 Sep 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
457	Anticipated international student revenue unrealised	Paul Ivey	<p>Cause: UK government process / policy changes. Restriction on current highly trusted sponsor status. Issues connected with english language test evidence. Anticipated TNE growth does not materialise.</p> <p>Effect: LSBU unable to organise visas for students who wish to study here. International students diverted to other markets. Expected income from overseas students unrealised. Conversion impact of LSBU TNE students doesn't materialise.</p>	<p>I = 3 L = 3 High (9)</p> 	Regular reporting of Visa refusal rates to Director of Internationalisation by Immigration Team.	<p>I = 3 L = 2 High (6)</p> 	Paul Ivey	Lead development of an LSBU partnership model for International activity.	28 Oct 2016
					<p>International Office runs annual cycle of training events with staff to ensure knowledge of & compliance with UKVI processes.</p> <p>Recruitment Reports presented to each meeting of Ops Board.</p>		Paul Ivey	Induct new Director of Internationalisation into role and organisation.	28 Oct 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
517	Impact of EU Referendum result on operating conditions & market trends	David Phoenix	<p>Cause: Following the vote to 'Leave', the Government is working towards a plan to extract the UK from the European Union. Whilst we appear to be a long way from the triggering of article 50, itself a 2 year process, the news of the outcome of the plebiscite has already seen impact in markets and international opinion.</p> <p>Effects: Staff impact: The outcome could impact on the ability of some existing staff to remain in the UK, and could impair the ability for future recruitment, both from Europe, and from other overseas territories.</p> <p>Recruitment impact: Currently EU students pay home fees & can access the UK student loan system. It is likely that higher fees and removal of this access will have a significant impact on the appeal of the UK to European applicants long term. Additionally the reporting of the Brexit outcome is having a negative impact on the reputation of the UK as a welcoming destination. These impacts on the sector could also cause changes in recruitment patterns at well-ranked institutions, which could have a negative impact on applicant pools elsewhere.</p> <p>Research Funding: Leaving the EU is likely to remove the ability of LSBU to partner in EU research projects, and access Horizon 2020 funding opportunities.</p> <p>Legislative Compliance: There could be additional administration cost in updating many EU compliant processes if regulations are..</p>	<p>I = 2 L = 3 Medium (6)</p>			David Phoenix	Continue to monitor closely, through UUK and other sector bodies, the potential impacts and responses.	31 Jul 2017
							Gurpreet Jagpal	Review bid development strategy in Research, and seek to find alternatives to offset any anticipated shortfalls from European sources.	31 Jan 2017
							Mandy Eddolls	Monitor situation with regard to employment law and right to work, and ensure that appointments are made in compliance with any changes to regulation.	28 Jul 2017

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
1	Failure to position LSBU to improve reputation & effectively respond to policy changes & shifts in competitive landscape	David Phoenix	<p>Causes:</p> <ul style="list-style-type: none"> - Changes to fees and funding models - Increased competition from Private Providers - TEF and Apprenticeship development - Failure to anticipate change - Failure to position (politically) - Failure to position (capacity/structure) - Failure to improve League Table position <p>Effects:</p> <ul style="list-style-type: none"> - Failure to recruit students - Failure to differentiate 	I = 4 L = 3 Critical (12)	Ketchum appointed to advise LSBU on the ongoing changes to the political environment for higher education & its external communications in response to these changes.	I = 4 L = 1 High (4)	Shan Wareing	Oversee preparation of Narrative reports element of submission to the TEF.	23 Dec 2016
					<p>Financial controls (inc. forecasting & restructure) enable achievement of forward operating surplus target communicated to Hefce in July Forecast.</p> <p>The Business Intelligence Unit (BIU) provides Senior Managers with trend analysis and competitor benchmarking on all KPIs</p> <p>A horizon scanning report produced by the Policy Unit</p> <p>Maintain relationships with key politicians/influencers, boroughs and local FE</p> <p>Annual review of corporate strategy by Executive and Board of Governors</p>		Michael Simmons	Fully populate team within newly created Office of Corporate Affairs.	31 Jan 2017

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
362	Low staff engagement impacts performance negatively	Mandy Eddolls	<p>Causes:</p> <ul style="list-style-type: none"> •Bureaucracy involved in decision making at the University •No teamwork amongst departments at the University •Staff feeling that they do not receive relevant information directly linked to them and their jobs •Poor pay and reward packages •Poor diversity and inclusion practises <p>Effects:</p> <ul style="list-style-type: none"> •Decreased customer (student) satisfaction •Overall University performance decreases •Low staff satisfaction results •Increased staff turnover •Quality of service delivered decreases 	I = 3 L = 3 High (9)	Cascade messages from Ops Board circulated for Cascade Meetings within each School & Professional Function.	I = 3 L = 2 High (6)	Cheryl King-McDowall	Deliver a planned programme of activities to ensure continued awareness raising and promotion of the Behavioural Framework, to embed the values in to HR documentation, and to develop baseline measures.	30 Sep 2016
					Departmental Business Planning process		Markos Koumaditis	Complete progress review of University, School & PSG action plans.	28 Feb 2017
					Direct staff feedback is encouraged through the "asktheVC@" email address and through feedback forms on intranet and 'developing our structures' microsite.		Cheryl King-McDowall	Conduct EES Pulse survey for key themes.	31 May 2017
					Scheduled Team meetings		Jo Sutcliffe	Complete soft launch of new staff intranet.	31 Oct 2016
					Regular Business review meetings				

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
2	Revenue reduction if marketing and admissions process does not achieve Home/EU recruitment targets	Ian Mehrtens	<p>Causes:</p> <ul style="list-style-type: none"> - Changes to UGFT fees - Increased competition (removal of SNC cap in 15/16) - Failure to develop and communicate brand & lsbu graduate attributes - Lack of accurate real-time reporting mechanisms - Poor league table position - Portfolio or modes of delivery do not reflect market need - Tighter tariff policy during clearing <p>Effects:</p> <ul style="list-style-type: none"> - Under recruitment - loss of income - Loss of HEFCE contract numbers - to 14/15 - Failure to meet related income targets - cost of legal challenge relating to CMA guidance 	I = 4 L = 3 Critical (12)	<p>Report on student applications is presented to every monthly meeting of Operations Board & reviewed by Board of Governors</p> <hr/> <p>Weekly Report linking student numbers to anticipated income levels circulated to Ops Board.</p> <hr/> <p>Advance predictions of student recruitment numbers informs the Annual five year forecast submitted to Hefce each July</p> <hr/> <p>Differentiated marketing campaigns are run for FTUG, PTUG and PG students on a semesterised basis.</p>	I = 4 L = 2 Critical (8)	Pat Bailey	Oversee Executive scenario planning activity, to explore growth opportunities within portfolio, and to consider action in the event of an income shortfall.	30 Dec 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
3	Staff pension scheme deficit increases	Richard Flatman	<p>Causes:</p> <ul style="list-style-type: none"> - Increased life expectancies - Reductions to long term bond yields, which drive the discount rate - Poor stock market performance - Poor performance of the LPFA fund manager relative to the market - Impact of change from FRS17 to FRS102 - Further change to accounting requirements for TPS & USS schemes <p>Effects:</p> <ul style="list-style-type: none"> - Increased I&E pension cost means other resources are restricted further if a surplus is to be maintained - Balance sheet is weakened and may move to a net liabilities position, though pension liability is disregarded by HEFCE - Significant cash injections into schemes may be required in the long term - Inability to plan for longer term changes 	I = 3 L = 3 High (9)	<p>Regular monitoring of national/sector pension developments and attendance at relevant conferences and briefing seminars</p> <hr/> <p>Annual FRS 102 valuation of pension scheme</p> <hr/> <p>Regular participation in sector review activity through attendance at LPFA HE forum, & UCEA pensions group by CFO or deputy.</p> <hr/> <p>Regular Reporting to Board via CFO Report</p> <hr/> <p>DC pension scheme for SBUEL staff.</p> <hr/> <p>Tight Executive control of all staff costs through monthly scrutiny of management accounts</p> <hr/> <p>Strict control on early access to pension at redundancy/restructure</p>	I = 3 L = 2 High (6)			

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
6	Management Information is not meaningful, unreliable, or does not triangulate for internal decision or external reporting	Richard Flatman	<p>Causes:</p> <ul style="list-style-type: none"> - Lack of strategic vision for ICT - Proliferation of technology solutions - Data in systems is inaccurate - Data in systems lacks interoperability - Resource constraints & insufficient staff capability delay system improvement - Lack of data quality control and assurance mechanisms <p>Effects:</p> <ul style="list-style-type: none"> - Insufficient evidence to support effective decision-making at all levels - Inability to track trends or benchmark performance - Internal management information insufficient to verify external reporting - unclear data during clearing & over-recruitment penalties - League table position impaired by wrong data - Failure to satisfy requirements of Professional, Statutory and Regulatory bodies (NHS, course accreditation etc) 	I = 3 L = 3 High (9)	Data Assurance Group meets to review matters of data quality and provides reports to Operations Board.	I = 3 L = 2 High (6)	John Baker	Oversee delivery of the first product of the next phase of the MIO dashboard project - a visualisation of the enrolments data contained within the DARR report.	30 Sep 2016
				Internal Auditors Continuous Audit programme provides regular assurance on student and finance information, including UKVI compliance.	Mandy Eddolls	Deliver i-trent HR data system replacement	28 Feb 2017		
				<p>Engagement between International Office, Registry & School Admin teams to ensure UKVI requirement compliance, specifically regarding:</p> <ul style="list-style-type: none"> - Visa applications and issue of CAS - English language requirements - Reporting of absence or withdrawal <p>Systematic data quality checks and review of key data returns prior to submission by B.I.U.</p> <p>Sporadic internal audit reports on key systems through 3 year IA cycle to systematically check data and related processes:</p> <ul style="list-style-type: none"> - HR systems - Space management systems - TRAC - External returns 					



Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
14	Loss of NHS contract income	Warren Turner	<p>Cause: NHS financial challenges/ structural change is resulting in a total review of educational commissioning by Health Education England with an expected overall reduction in available funding (affecting CPPD).</p> <p>Plus London Educational Contracts (pre-registration) are running out from Sept 2017 with students paying their own fees via student loan system.</p> <p>Recruitment to contracted programmes is buoyant currently but could dip following shift from bursaries to tuition fees.</p> <p>Effect: Reduction in income Reduced staff numbers Reduced student numbers</p>	I = 3 L = 3 High (9)	<p>Named Customer Manager roles with NHS Trusts, CCGs and HEE.</p> <hr/> <p>Monitor quality of courses (QCPM and NMC) annually in autumn (QCPM) and winter (NMC)</p> <hr/> <p>Support with numeracy and literacy test preparation.</p> <hr/> <p>Complete review in 2016/17 of all post-registration/ PG and CPPD courses and modules to ensure these remain leading edge and fit for the future. Review programmed to involve all stakeholders and to be employer driven.</p>	I = 3 L = 2 High (6)	Anthony Mcgrath	Increase formal progression/ access partnerships with FE colleges and establish FE partner health & social care network to increase supply chain for FE-entrants to pre-reg education	31 Dec 2016
							Sue Mullaney	Improve NSS participation & scores Develop action plans for Departments and School from results of 2015 NSS	28 Feb 2017
							Warren Turner	Plan for renewal of Havering lease in 2018/19 or alternative site. Continue discussions with NHS partners in NE London (BHR, NELFT and Barts) together with Queen Mary School of Medicine and Dentistry re potential for revitalising the Harold Wood site for the future.	31 Dec 2016
							Anisa Salim	Provide clear, timely and accurate advice to potential students re change from bursaries to student loans through improvements to web site and at open days	30 Sep 2016
							Warren Turner	Grow into new markets for medical and private sector CPPD provision - include as part of Ipsos Mori bi-annual survey to identify workforce/ education requirements. Include these in CPPD course review	31 Dec 2016
							Sheelagh Mealing	Increase uptake in band 1-4 activity Support Trusts in seeking external (non NHS) funding Work with NHS partners to meet demand for apprenticeship programmes/ Foundation Degrees (esp around Assistant/ Associate Practitioner roles)	31 Mar 2017
							Anisa Salim	Develop a programme of open events held jointly with our NHS partners to ensure that we reach all sectors of the community re attracting the best pre-reg students for Sept 2017 and beyond	31 Dec 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
37	Affordability of Capital Expenditure investment plans	Richard Flatman	<p>Causes:</p> <ul style="list-style-type: none"> - Poor project controls - Lack of capacity to manage/deliver projects - Reduction in agreed/assumed capital funding - Reduction in other government funding <p>Effects:</p> <ul style="list-style-type: none"> - Adverse financial impact - Reputational damage - Reduced surplus - Planned improvement to student experience not delivered - Inability to attract new students 	<p>I = 3 L = 3 High (9)</p> 	<p>Management Accounts, with a CAPEX report section, are provided to each meeting of the FP&R Committee, and the Board receives business cases in relation to all planned capital expenditure > £1million.</p> <hr/> <p>Full Business Cases prepared; using guidance and process approved by Executive - including clarity on cost and funding, for each element of Estates Strategy, and approved by Board of Governors where cost = >£1M</p> <hr/> <p>Clear requirement (including authority levels) for all major (>£1m) capital expenditure to have Board approval</p> <hr/> <p>Major Projects & Investments Committee (MPIC) is a Board sub-committee with remit to review all property related capital decisions, and is empowered to approve all unplanned capital expenditure > £500K but <£1M.</p> <hr/> <p>Capex reporting routines established and embedded into regularly updated financial forecasts & management accounts and regular Board reports.</p>	<p>I = 3 L = 1 Medium (3)</p> 	Ian Mehrtens	Complete report on the final Student Centre negotiations. Update: the 12 month defects liability period concluded & working through the final defect list. POE was due by Feb 14.	30 Apr 2013
							Ian Mehrtens	Creation and submission of business case for wider estate development programme to MPIC Board Committee.	30 Nov 2016

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Person Responsible	Action Required	To be implemented by
					LSBU Project methodology & Estates & Facilities Dept project controls, including Governance arrangements applied to all Capex projects.				
305	Student & corporate data not accessed and stored securely or appropriately	Ian Mehrtens	<p>Cause: Loss or inappropriate access to data, or breach of digital security; either en masse (e.g. address harvesting) or in specific cases (e.g. loss of sensitive files / data)</p> <p>Effect: Reputational damage, regulatory failure, undermining of academic credibility or compromise of competitive advantage.</p>	I = 3 L = 2 High (6)	Responsibility for control over data protection risks at an institutional level allocated to Director of ARR (Academic Related Resources)	I = 3 L = 2 High (6)	Craig Girvan	Deliver project to ensure mandatory training is delivered to staff via ICT log on, to include data security awareness.	29 Jan 2016

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Risk Strategy – Revised Draft for Approval
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	John Baker – Corporate & Business Planning Manager
Executive sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with a revised Risk Strategy – for recommendation to the Board of Governors.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This Risk Strategy relates to the management of risks or uncertainties across the institution and which could impair the ability of the University to achieve all of the goals of the Corporate Strategy.
Recommendation:	Committee is requested to: <ul style="list-style-type: none"> • Recommend the revised Strategy to the Board for Approval (Along with the Risk Management Policy*)

Matter previously considered by:		On:
Further approval required?	Board of Governors	October 20 th 2016

Executive Summary

The revised Strategy builds on the document approved by the Board in June 2014.

The main changes from the previous Strategy are:

- The terminology has been updated to reflect the current structures and management review processes within the organisation, and the establishment of the new Strategic Risk Review Group
- The strategy has been revised to accommodate the additional functionality of the updated risk management software
- Operational aspects have been extracted into a risk management policy, which is provided as an appendix for information, along with a new assurance framework model
- Further information has been provided to respond to findings from previous internal audit reports, in regard to escalation process and process utility.

The Committee is requested to:

- Recommend the revised Strategy to the Board for Approval

Risk Strategy

Strategy Meta Data:

Originating Department:	Finance & Management Information
Enquiries to:	John Baker – Corporate & Business Planning Manager
Approving Committee/Body:	Board of Governors
Current Version No:	4
Last Approved:	Version 3 approved June 2014
Next due for approval:	October 2016
Document Type:	Strategy
Mandatory Target Audience:	Risk Champions (University Executive), School Management, Professional Service Group Managers
Also of Relevance to:	All staff
Brief Summary of Purpose:	The Risk Strategy sets out the University's approach to risk management. It sets out the roles and responsibilities of the Board of Governors, the Executive, and other key parties. It also sets out risk management and reporting processes, and links with corporate and business planning.

Risk Strategy sections

Section A: Strategy Purpose	1
Section B: Risk management & Governance	2
Section C: Risk Management – Overview	2
Section D: Risk Management – Responsibilities	5
Section E: Risk Management – Software	6
Section F: Corporate Risk	6
Section G: Operational Risk	7

Appendix 1: Risk Management Policy

Section A: Risk Management – Process	9
Section B: Risk Priority & Rating Methodology	10

Appendix 2: Risk Assurance 3 Lines Framework 12

Appendix 3: Risk Hierarchy Diagram & table 14

A: Purpose of the Risk Strategy

1. The Risk Strategy explains the University's approach to risk management. Risk Management provides a mechanism and framework which at the highest level seeks to ensure that the University achieves its strategic objectives, through effective identification, and management of uncertainties that could impact on these outcomes.
2. It is also a key requirement of the Hefce Memorandum of Assurance and Accountability, which defines the operating aspects of effective management in which all Higher Education providers must operate.
3. The Risk Strategy sets out the roles and responsibilities of the Board of Governors, the Executive and other key parties. It also sets out the risk management process at LSBU and the main reporting procedures.
4. The Risk Strategy is part of the University's **internal control** and **corporate governance arrangements**.

B: Risk management & governance

5. The University is committed to the highest standards of corporate governance. This risk strategy and the processes set out herein form an important part of LSBU's governance arrangements.
6. The Risk Strategy is approved by the Executive, the Audit Committee, and the Board of Governors.
7. The Board of Governors also has a fundamental role to play in setting the risk appetite of the University, and in oversight of the management of risk. Its role is to:
 - Approve the risk appetite of the University both as a whole and on any relevant individual issue (or risk type).
 - Approve the policy in relation to risk management
 - Approve major decisions affecting the University's risk profile or exposure
 - Approve, on an annual basis, the corporate risk strategy

- Review annually the risk management arrangements
- Delegate matters as required to the Audit Committee, including assurance provided through the annual Internal Audit programme.
- Review at each meeting the corporate risk register

C: Risk Management – Overview & Objectives

8. For the purpose of risk management, risk is defined as

“The threat or possibility that an action or event will adversely affect LSBU’s ability to achieve its objectives”.

9. This could be any event, outcome or action which could:

- Cause financial disadvantage to the University, i.e. loss of income, additional costs, loss of assets, creation of liabilities
- Cause damage to the reputation of the University
- Prevent an opportunity from being taken
- Lead to a failure to capitalise on our strengths
- Prevent or hinder achievement of any of the objectives of the Corporate Strategy or associated local delivery plans
- Impact negatively on student experience or achievement

10. Risk management is the process of identifying, defining and analysing these risks, and deciding on an appropriate course of action to either minimise the potential impact of these risks, or to establish controls to reduce the likelihood of their occurrence, to ensure that these risks do not impair the achievement of objectives at the relevant level.

11. To be effective, risk management needs to be embedded into the culture and processes of the University. Risk management affects everyone in the University and therefore all staff should be aware of this document and be familiar with the principles and procedures it contains.

12. This Risk Strategy document and the Risk Appetite statement will be made available on the staff intranet, and the LSBU approach to risk management will be included in the induction resources provided to new managers and staff by

the OSDT team, and included on the agenda of the biannual 'Welcome to the University' conference events organised for new starters.

Risk Management – Objectives

13. The higher level risk management objectives of the University are to:
- Integrate risk management into the culture of the University
 - Ensure that necessary risk management procedures are embedded into the University's management, and governance processes
 - Manage risk in accordance with best practice
 - Support key business decisions through embedded risk appraisal processes
 - Effectively manage existing risks within agreed risk tolerances
 - Anticipate and respond to changing social, environmental, legislative and other requirements

D: Risk Management - Responsibilities

14. *Executive:*
The Executive is responsible for ensuring that the risk management process operates effectively, that key risks are identified, that appropriate controls or other mitigating actions are in place and that matters are escalated and reported to Board as considered appropriate. The Executive will also own all Corporate Risks.
15. *Operations Board:*
The Operations Board is responsible for ensuring that the risk management procedures are carried out effectively, and that key corporate risks are identified, and managed effectively. Corporate Risk management will be a standing agenda item at quarterly Operations Performance Review meetings, and members also have a responsibility to escalate matters from operational registers as appropriate.
16. *Strategic Risk Review Group:*
In addition to the regular reviews of the Corporate Register Operations Board, The Strategic Risk Review Group, a sub-group of the Executive, with other colleagues from across the institution, will meet on three occasions each year, in

January, May and September, ahead of the meetings of Audit Committee, to review strategic risk matters, and the operation of this strategy.

17. *Risk Champions:*

All members of the Executive are Risk Champions for their areas of the University and will have overall responsibility for the adequacy and effectiveness of the risk management processes in their areas of operation. These responsibilities are clearly set out in their letters of delegated authority.

Risk Champions may delegate responsibility for risk management in particular areas to the heads of those areas via the letters of delegated authority.

Risk Champions retain overall responsibility for:

- Ensuring that risks are identified and reviewed alongside Local Delivery Plans by the relevant risk owners
- Ensuring that risk management is carried out in accordance with this strategy
- Reviewing and reporting any significant changes in risk exposure
- Escalating operational risk matters through the Operations Board as appropriate

18. *Risk Owners:*

Risk Owners are responsible for the management of specific corporate and/or operational risks. All Corporate risks must be owned by a member of the Executive, but operational risks may be owned by any member of staff as nominated by the appropriate Risk Champion.

Risk Owners take responsibility for the management of the risk, including:

- Identification of controls and management actions
- Implementation of controls and management actions
- Continued awareness and monitoring of any changes in the likelihood or impact of each risk
- Review of any objectives or performance indicators associated with the risk

19. *All staff:*

All members of staff have a responsibility to be risk aware, to ensure that this risk management strategy is observed in their daily work, and that any potential new areas of risk that they identify are reported to their line manager or Risk Champion in a timely manner.

20. *Link to other responsibilities: Health & Safety*
All staff, students and other workers have a responsibility to observe the stipulations of the University's approach to the management of Health & Safety. This includes assessment of personal risk whilst within the campus environment, and is covered by the policies and work of the Health & Safety Committee. This is not within the remit of this strategy, which is focused on risks to the achievement of management objectives.
21. *Decision Making:*
The Risk Management Records maintained and updated in line with this strategy are used by the institution in the formal processes identified within it to both consider the adequacy of existing activity in line with objectives at all levels, and to consider issues of business development, the allocation of resources and response to changing conditions in the operational environment.

E: Risk Management - Software

22. The University uses a web-based system called 4Risk, which is part of the Insight 4 Governance Suite (available via <http://kepler/Risk/Home.aspx>) to record and report all risk management activity.
23. All Risk Champions will be able to access training in the use of 4Risk, and should use the software to update management activity against the corporate risks they own, and oversee its use in the operational areas which they manage.
24. Any requests for training in the use of 4-Risk, should be directed to the Corporate & Business Planning Manager (on extension 6360).
25. Any technical problems with access to the platform should be directed to the ICT heldesk support function via extension 6500 or via <https://ict-helpdesk.lsbu.ac.uk/>

F: Corporate Risk

26. Corporate risks are those which could cause financial or reputational damage to the University as a whole, or prevent or hinder the achievement of Corporate Plan objectives. Each corporate risk is owned by a member of the Executive.

27. The corporate risk register will be used to determine the focus of the annual internal audit plan.
28. Corporate Risks must be owned by a member of the Executive, and each risk entry will:
 - Provide details of the impact and likelihood of the risk identified;
 - Indicate who is responsible for the management of the risk;
 - Identify the key controls in place to manage each risk;
 - Provide an assessment of the inherent and residual exposure of each risk; and,
 - Identify the actions required to manage the exposure to each risk.
29. Assessment of corporate risk exposure should be monitored continuously by Executive leads, and will be reviewed 3 times a year at the regular performance & progress review meeting of the Operations Board.
30. The current Corporate Risk register should be reported to each meeting of the Audit Committee and the Board of Governors.
31. Any corporate risk that is rated 'Low' should be considered for downgrading to the appropriate Operational Risk Register. The Operations Board are responsible for downgrading corporate risks through the normal cycle of meetings.
32. The Risk Appetite statement provides an approach to assessment of the level of risk within which the Corporate Risk is managed for the institution, and is reviewed annually.
33. The risks in the Corporate Register are allocated to the goals of the Corporate Strategy, and the Strategic Risk Review Group will consider the objectives and their associated risks as a standing agenda item at their meetings.
34. We should expect there to be real linkage between the risks to delivery of Corporate projects, which by their nature address key strategic issues, and the Corporate risks for the institution. The delivery of Corporate projects will be monitored regularly by the Executive, and reported to the Board of Governors. It is the responsibility of the Executive to ensure that the risk registers for projects are kept up to date, and that the Corporate Risk Register is updated in a timely way to reflect any changes to project deliverables.

G: Operational Risk

35. Operational risks could prevent achievement of School and Professional Service Group objectives, as identified in Local Delivery Plans for these areas.
36. An operational risk register is maintained by each School and by each Professional Service Group. It is the responsibility of the relevant Executive member, in their role as Risk Champion for their own area of responsibility, to ensure that these operational risk registers are maintained by the management teams within each School and PSG.
37. Management of individual operational risks may be delegated within each area as appropriate. Where responsibility for operational risk management is delegated, this should be to a named individual who will be known as a Risk Owner.
38. The impact and likelihood of each operational risk is rated using the same methodology as that applied to corporate risks.
39. All operational risks with a 'critical' risk priority should be referred to the Operations Board for consideration, and potential escalation to the corporate risk register.
40. Risk Champions are responsible for escalating operational risks. Escalation is through the normal cycle of Operations Board meetings although matters of a more fundamental nature should be reported immediately.
41. Fundamental Risks: These are risks which have a risk severity rating of critical, and which threaten the immediate safety of students or staff, or the financial standing or reputation of the institution.
42. More formal review of Operational risk registers will take place through the Executive Review Meetings, which take place at the midpoint of the academic year.

Risk Management and Business Planning

43. Planning and budgeting at an Operational level (School and Professional Service Group) takes place on an annual basis, with Local Delivery Plans for each area

developed through the annual Planning & Budgeting process and reviewed and approved alongside budgets prior to the start of the next academic year.

44. The Local Delivery Plan template requires managers to identify and prioritise their top 3 risks or challenges, and to identify mitigating actions. These top three risks should be included in the relevant operational risk register and, together with any other operational risks, should be reviewed and updated according to the usual process.

Regular Review of Operational Risk Management

45. Risk Management should be a regular agenda item in the management meetings within School Executive Teams, and within the Management meetings of Professional Service Groups.
46. Risk management will be a standing agenda item at all of the Annual Executive Review Meetings, where Risk Registers, with details of risks and mitigating actions, will be reviewed alongside progress against the delivery of plans, KPIs and financial performance.
47. The Risk Review Functionality of the 4-Risk platform will be configured to require all risk owners to log into the system at 3 points during each year and check that the risk entries for which they are responsible are up to date. (in February, June, & October)
48. The Strategic Risk Review Group will also meet 3 times a year, and will consider strategic risk elements drawn from registers across the institution as part of its regular agenda.
49. Risk Management also features as a mandatory topic within the annual internal audit programme, and at the end of each financial year, a sample of operational registers will be selected to feed into this piece of audit activity, in order to provide 3rd party assurance as to the effectiveness of this risk strategy.
50. Mitigating actions identified in operational risk registers should be cross-referenced to the deliverables identified in Local Delivery Plans and reviewed alongside delivery of those actions and projects.

London South Bank University: Risk Management Policy

Section A: Risk Management - Process

1. The University has adopted a two tier system to risk management, with risks defined at one of two levels, either Corporate or Operational.
2. *Corporate risks*: could cause financial or reputational damage to the University as a whole, or prevent or hinder the achievement of the objectives within the Corporate Strategy.
3. *Operational risks*: could prevent achievement of School and /or Professional Service Group objectives as set out in respective local delivery plans.
4. The risk management process as set out below applies to both corporate and operational risks.
5. The key stages of the risk management process are as follows:
 - **Identify the risks** which prevent or hinder the achievement of the corporate plan and/or operational business plan objectives. This should be done on a continual basis and reviewed regularly.
 - **Assess the potential impact and inherent likelihood** of each risk to give a total risk priority of low, medium, high or critical. See section I on “Risk Priority: Rating methodology” for details of this system. The inherent priority should represent the potential impact and the likelihood of the risk occurring if there were no controls in place
 - **Consider whether there are existing controls** that are in place. Controls are ongoing auditable processes or regular checks or scrutiny that serve to reduce the impact of the risk and/or the likelihood of occurrence
 - **Identify any required actions** that should be taken by management to reduce the potential impact or likelihood of the risk occurring
 - At this stage **record the risk details** in the online 4-Risk [Platform](#) for the risk area under consideration.

- If there are controls in place **assess the residual likelihood** of the risk to give a second risk priority rating. The residual priority should represent the impact and likelihood after all controls have been taken into account, and can be expected to be lower than the inherent rating if the controls are effective.
- **Implement any identified actions** to reduce residual impact/likelihood to an acceptable level,.
- **Record and amend the actions** taken by management in the online platform
- **Regularly review risk registers**, which provide a snapshot of the risk records in any given area at a particular point in time.

Section B: Risk Priority - Rating methodology

6. Risks are measured in terms of their impact and likelihood. A measurement should be made of both the inherent and residual risk.

Impact

- *Critical* – occurrence would have a critical effect on the ability of the University to meet its objectives; could result in the removal of degree awarding status, removal of funding, severe reprimand by HEFCE or Parliament or the closure of the University.
- *High* – occurrence would have a significant effect on the ability for the University to meet its objectives and may result in the failure to achieve one or more corporate objectives.
- *Medium* – occurrence may result in the failure to meet operational objectives and may reduce the effectiveness of the University but it would not result in the failure of the University’s corporate objectives or put the University as a whole at risk.
- *Low* – occurrence would have little effect on operational or corporate objectives.

Likelihood

- *High* – likely within 1 year
- *Medium* – may occur medium to long term
- *Low* – unlikely to occur

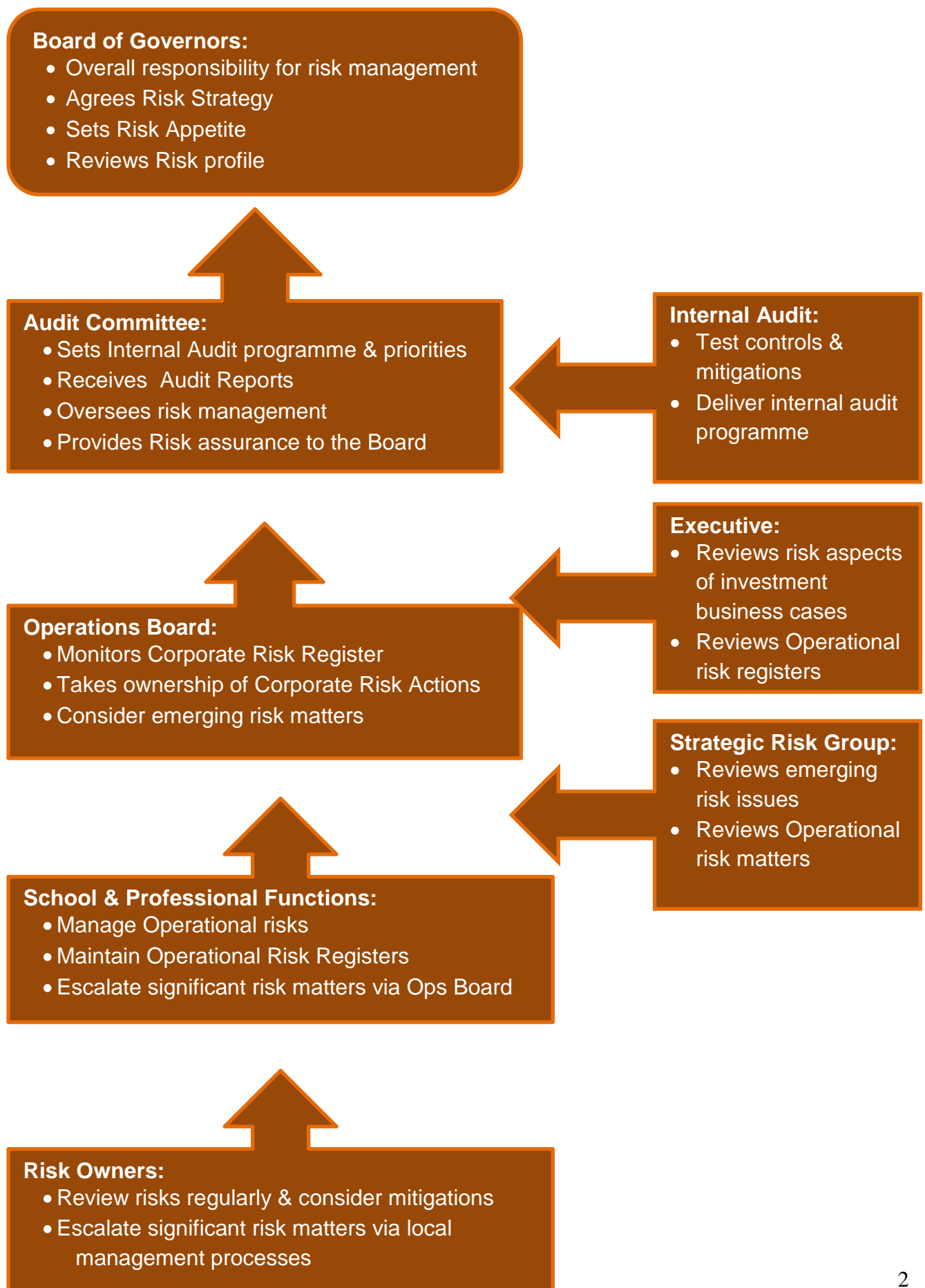
Table 1: Total Risk Values based on assessment of impact and likelihood

Impact	4 - Critical	High	Critical	Critical
	3 - High	Medium	High	High
	2 - Medium	Low	Medium	Medium
	1 - Low	Low	Low	Low
		1 - Low	2 - Medium	3 - High
		Inherent Likelihood		

LSBU Risk Management Assurance Overview: 3 lines of Defence, including Risk Appetite risk categories

Risk Area	Line 1 (Staff & Technology, Process & Procedures)	Line 2 (Management Oversight)	Line 3 (Independent Assurance)	Controls / Notes
LSBU – Institutional Risk Management	Individual Review: Online (every 4 months, by Risk Owners) Structural Review: School and Professional Function Management meetings (occasional)	Corporate Risk: Operations Board & Strategic Risk Review Group: (3 times a year) Operational Risk: Executive Review Meetings (Each February)	Internal Audit Programme: Risk Management Report (Each July – as per Hefce Memorandum)	Risk Strategy – see Risk Framework Document
Risk Types:				
Financial	Financial Regulations Procure2Payment invoice process automation Procurement checks	Financial Controller Head of Procurement Capital Investment approval process	Internal Audit: Continuous Audit programme External Audit Procurement maturity assessment	Key component of annual internal audit programme.
Legal / Compliance	Staff compliance with policies and procedures Mandatory training programme within ODT	Legal Support from Legal & Governance team	3 rd Party Expertise on specific matters <ul style="list-style-type: none"> • Shakespeare Martineau LLP • Veale Wasborough Vizards LLP • Shoosmiths LLP • Eversheds LLP 	Mandatory staff training programme includes: <ul style="list-style-type: none"> • Recruitment & Selection • Data Protection & FOI • Health & Safety Awareness • Equality & Diversity
Academic Activity	Quality Office & related curriculum cycles Centre for research informed teaching & digitally enhanced learning	Academic Board	Internal Audit: Specific Audits QAA Review	Planned through yearly risk review process by AQDO.
Reputation	PR & Internal Comms Teams Incident Response Team Town Hall Cascades	League table working group Leadership Forum	Hefce 5 year institutional review	Ketchum contract works to develop contacts and insight. Policy Unit leads institutional stakeholder engagement.

LSBU Risk Framework: Diagrammatic Overview of Risk Strategy Elements



LSBU Risk Overview – Risk Framework: Levels of Review Table

<i>Level of Review</i>	<i>Activity</i>	<i>Format of Review</i>	<i>Frequency</i>	<i>Details / notes</i>
Hefce	Institutional Risk Assessment	Risk Letter in March	Yearly	Utilises data from Dec AAR return and signed accounts
Board of Governors	Detailed Risk Review	November meeting	Yearly	Papers on Governors Drive
	Consideration of risk matters	Strategy Days	Six monthly	Strategy agendas
	Noting of Register	Paper at Meetings	5 per year	Papers on Governors Drive
Audit Committee	Risk Review	Paper at Meetings	4 per year	Papers on Governors Drive
Executive:	Operational Risk Review	Register at Feb Executive Review Meetings	Yearly	Papers stored in EXEdrmd drive
	Business Case Review	Business Cases above defined thresholds	When submitted	Risk section within template
Operations Board:	Corporate Risk Review	Register noted at Meetings	Monthly	Papers in Exec folder
Strategic Risk Review Group:	Review of risk matters	Exec sub group meeting with key risk representatives	Three times per year	Managed by FMI function
Schools & Professional Functions:	Risk consideration	Risk matters incorporated into local management meetings	Monthly / Quarterly	Local control of agendas
	Operational Risk Review	Register at Feb Executive Review Meetings	Yearly	Papers stored in EXEdrmd drive
	New Risk Consideration	Section of planning template submitted in June	Yearly	Registers linked to local objectives
	Risk Owner Review	Online Risk platform review process	Three times per year	http://kepler/
Members of Staff:	Issue raising	local management meetings	Ad hoc	Local minutes

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Risk Appetite – Statement for Approval
Board/Committee	Audit Committee
Date of meeting:	22 nd September 2016
Author:	John Baker – Corporate & Business Planning Manager
Executive sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	To provide Committee with a Risk Appetite statement – for recommendation to the Board of Governors for 2016/17.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	The Risk Appetite relates to the management approach towards matters of risk, and provides a context in which decisions are made by the University in its actions intended to impact on all goals of the Corporate Strategy.
Recommendation:	Committee is requested to: <ul style="list-style-type: none"> • Recommend the Risk Appetite statement to the Board for Approval

Matter previously considered by:	Strategic Risk Review Group	On: 6 th September 2016
Further approval required?	Board of Governors	October 2016

Executive Summary

The Risk Appetite statement was approved by the Board in June 2015.

The statement was reviewed by the Strategic Risk Review Group, and their recommendation to Committee is to maintain the risk appetite statement at current levels. This is because:

- It has now been embedded within current processes
- There have been no significant changes to the Corporate Strategy, and the financial strategy, which would require a change to approach.

The Committee is requested to:

- Recommend to the Board that the current Risk Appetite statement remains in operation for the academic year ahead.

London South Bank University Risk Appetite: Agreed Statement – June 2015

The risk appetite statements agreed by the Board were as follows for each risk type:

- a. Financial – open;
- b. Legal and compliance – cautious;
- c. Academic delivery – seek;
- d. Reputational – open.

These are displayed against the original framework overleaf, with descriptive statements.

Embedding the Risk Appetite into Institutional Activity:

Page 262

The risks on the Corporate Risk Register have been cross referenced with the appetite risk types, as in the image on the left from the Board Strategy Day in April 2016, to consider exposure by type.

- The risk categories have been inserted into a draft revision of the business case template, to enable consideration of investment ideas in conjunction with risk appetite as part of the institutional change or investment appraisal process.
- The Risk Appetite was used to consider and develop the Internal Audit Plan for 2016/17, to ensure that assurance provided covers the stated risk approach.

Severity Rating	Critical	High	Medium	Low
Risk Types:				
Financial (Open)	2: Revenue reduction if marketing and PR activity does not achieve H/EU UG recruitment targets (IM)	457: Anticipated international student revenue unrealised (PI) 14: Loss of NHS contract income (WT) 3: Increasing pensions deficit reduces flexibility (RF) 402: Income growth from Research & Enterprise unrealised (PI)	37: Affordability of Capital Expenditure investment plans (RF)	
Legal / Compliance (Cautious)		305: Data not used / maintained securely (IM)		
Academic Activity (Seek)		6: Management Information perceived as unreliable, doesn't triangulate or is not presented (RF) 467: Progression Rates don't increase (PB) 495: Higher Apprenticeship degrees (PB)	398: Academic programmes not engaged with technological and pedagogic developments (SW) 494: Inconsistent delivery of Placement activity across the institution (SW)	397: Effectiveness of delivery impaired by restructuring process (DP)
Reputation (Open)		1: Lack of capability to respond to policy changes & shifts in competitive landscape (DP) 362: Low staff engagement impacts performance negatively (DP)		

Options	Avoid / Averse Avoidance of risk and uncertainty is a Key Organisational objective	Minimal (as little as reasonably possible) Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential	Cautious Preference for safe delivery options that have a low degree of inherent risk & may only have limited potential for reward	Open Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)	Seek Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)	Mature Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
Financial	Avoidance of financial loss is a key objective.	Only prepared to accept the possibility of very limited financial loss if essential.	Prepared to accept possibility of some limited financial loss. Resources generally restricted to existing commitments.	Prepared to invest for return and minimise the possibility of financial loss by managing the risks to a tolerable level. Resources allocated in order to capitalise on opportunities.	Investing for the best possible return and accept the possibility of financial loss (with controls may in place). Resources allocated without firm guarantee of return – 'investment capital' type	Consistently focused on the best possible return for stakeholders. Resources allocated in 'social capital' with confidence that process is a return in itself.
Legal Compliance	Play safe; avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge. Similar situations elsewhere have not breached	Limited tolerance for sticking our neck out. Reasonably sure of addressing any challenge.	Challenge would be problematic but we are likely to win it and the gain will outweigh the adverse consequences.	Chances of losing any challenge are real and consequences would be significant. A win would be a great coup.	Consistently pushing back on regulatory burden. Front foot approach informs better regulation.
Academic Activity	Defensive approach to objectives – aim to maintain or protect, rather than innovate. Priority for tight management controls & limited devolved authority. General avoidance of systems/ technology developments.	Innovations always avoided unless essential or commonplace elsewhere. Decision making authority held by senior management. Only essential systems / technology developments to protect current operations.	Tendency to stick to the status quo, innovations in practice avoided unless really necessary. Decision making authority generally held by senior management. Systems / technology developments limited to improvements to protection of current operations.	Innovation supported, with demonstration of commensurate improvements in management control. Systems / technology developments used routinely to enable operational delivery. Responsibility for non- critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' & challenge current working practices. New technology viewed as a key enabler of operational delivery. High levels of devolved authority; management by trust rather than tight control.	Innovation the priority – consistently 'breaking the mould' and challenging current working practices. Investment in new technologies as catalyst for operational delivery. Devolved authority – management by trust rather than tight control is standard practice.
Reputation	No tolerance for any decisions that could lead to scrutiny of, or indeed attention to, the organisation. External interest in the organisation viewed with concern.	Tolerance for risk taking limited to those events where there is no chance of any significant repercussion for the organisation. Senior management distance themselves from chance of exposure to	Tolerance for risk taking limited to those events where there is little chance of any significant repercussion for the organisation should there be a failure.	Appetite to take decisions with potential to expose the organisation to additional scrutiny/interest. Prospective management of organisation's reputation.	Willingness to take decisions that are likely to bring scrutiny of the organisation but where potential benefits outweigh the risks. New ideas seen	Track record and investment in communications has built confidence by public, press and politicians that organisation will take the difficult decisions for the right reasons with benefits

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Annual review of effectiveness: Statement of Internal Controls
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	John Baker, Corporate & Business Planning Manager
Executive/Operations sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	To set out the full compliance statement on internal control for approval and inclusion in the year-end financial accounts and to set out the assurance sources in support of the full compliance statement.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	This statement relates to controls and processes that relate to the entire organisation, and its operating effectiveness.
Recommendation:	The Executive recommends that Committee: <ul style="list-style-type: none"> • Notes this report • Approves the annual compliance statement (subject to final review immediately before approval of accounts).

Matter previously considered by:	Executive	On: 14 th September
Further approval required?		

Executive Summary

This paper presents the annual review of effectiveness of the University's system of internal control, and underpins the internal control statement in the annual report and accounts. This paper is in draft form at this stage, until the approval of the financial statements, and will require further confirmation that no changes are required at the next meeting on the 10th November.

The proposed statement is a "full compliance" statement for the period under review. Please refer to section 1 of the report for the summary/justification of the full compliance statement.

- The Committee is requested to note this report, and approve the annual compliance statement.

London South Bank University

System of Internal Controls

Annual Review of Effectiveness
Year ended 31 July 2016

CONTENTS

1. Executive Summary
2. Annual review process
3. Changes in the nature and extent of significant risks
4. Scope and quality of management's ongoing monitoring of risks and the system of internal control
5. Results of internal audit work
6. Extent and frequency of communication to the board (and other committees)
7. Incidence of significant control failings or weaknesses during the year
8. Effectiveness of the University's external reporting processes

Appendix

1. Draft Statement on Internal Control
2. Corporate Risk Register Residual Likelihood Matrix Overview, as at 12th September 2016

1. Executive Summary

This report documents the progress that has been made to our system of internal control and to our risk management processes over the past year. A copy of the proposed statement of full compliance for the year ended 31 July 2016 is enclosed as Appendix 1.

In making this statement, we are required to ensure that a number of key principles of effective risk management have been applied. These principles, together with an assessment of compliance by LSBU, are provided in the table below.

Effective risk management:

Requirement	Assessment
Covers all risks – governance, management, quality, reputation and financial.	✓
Produces a balanced portfolio of risk exposure.	✓
Is based on a clearly articulated policy and approach.	✓
Requires regular monitoring and review, giving rise to action where appropriate.	✓
Needs to be managed by an identified individual and involves the demonstrable commitment of governors, academics and officers.	✓
Is integrated into normal business processes and aligned to the strategic objectives of the organisation.	✓

In making this assessment and a full compliance statement for the period under review (for the year ended 31 July 2016 and up to the date of approval of the financial statements) the following assurance sources have been taken into account:

HEFCE

- The most recent risk assessment, as reported by HEFCE in its letter to LSBU dated 4th March 2016 (and as reported to Board and Audit Committee at subsequent meetings) confirms that LSBU is “not at higher risk at this time”. The Executive is not aware of any issues which would currently change that rating
- HEFCE carried out an assurance visit to LSBU on 12 July 2011, which is conducted every 5 years. The overall conclusion from that review was the highest assurance rating possible “*that, at this time we (HEFCE) are able to*

place reliance on the accountability information.” No additional recommendations for improvement were included in the report.

Internal Audit

- The programme of internal audit work for the year ended 31 July 2016 was aligned to the corporate risk framework to provide assurance on the effectiveness of controls in key risk areas.
- The 2015/16 internal audit programme included a review of risk management. Based on the results, our risk processes were categorised as low risk. Corporate Risk was reported on a monthly basis to the University Operations Board and to every meeting of the Board of Governors and Audit Committee.
- The conclusions from internal audit work are discussed in more detail in section 5 of this report. There have been no critical findings this year.
- The opinion of the internal auditors is that controls are generally satisfactory, with some improvements required.
- The annual internal audit report outlines a small number of high risk findings which were raised regarding data security, but these do not present systemic threats to the entire control and governance environment. Appropriate action is being taken to address those weaknesses and to implement agreed actions.
- The overall number of findings has declined which indicates that there has been an improvement in the control environment compared to the previous year. Although the number of medium risk findings has increased by two, the number of high risk rated findings has decreased by two. The number of low risk rated findings have decreased significantly and there remains no critical findings.
- The overall internal audit action implementation rate for 15/16 was 88 % of all recommendations made. This is an improvement on the 83% reported last year, and above the benchmark target of 75%.

Internal Governance

- The Corporate Risk Register is aligned to the Corporate Strategy and is reviewed by Operations Board on a monthly basis and updated regularly. It has been re-structured to align to the new corporate strategy 2015/2020.
- The Corporate Risk Register has been submitted to every meeting of the Board of Governors and Audit Committee.
- In addition to the Risk Register, regular reports have been submitted to Audit committee/Board demonstrating progress on change projects and actions related to key corporate risks as appropriate.

- The Strategic Risk review Group has now been re-constituted with a formal Terms of Reference and a wider composition, and meets formally at 3 points in the academic year.
- Our opinion that LSBU's risk management arrangements continue to be strong is confirmed by the internal auditors in their annual review of risk management.
- There have been no major breakdowns in controls during the year. The annual internal audit opinion comments that the core financial control environment has remained robust during the year.
- Regular anti-fraud, bribery and corruption updates/reports have been provided to each meeting of the Audit Committee. No significant matters have occurred.
- No significant issues have arisen as a result of the University's external reporting processes.

2. Annual Review Process

To be able to make the statement on internal control set out in Appendix 1, Governors need to satisfy themselves that the risk management system is functioning effectively and in a manner that they have approved.

The two elements of effective monitoring are:

- An ongoing review process; (for LSBU this takes the form of regular risk management reports to the Audit Committee and Board of Governors, and ongoing monitoring reports and consideration of risk issues by the Operations Board); and
- An annual assessment of the effectiveness of internal controls.

This paper documents the annual assessment undertaken. It considers issues dealt with in reports received during the year, together with any additional information necessary to ensure that Governors take account of all significant aspects of internal control for the year under review and up to the date of approval of the annual accounts.

3. Changes in the nature and extent of significant risks

The Corporate Risk Register has been subject to monthly review by the Operations Board and has been updated as appropriate. The Risk Register has been aligned with the goals of the University's Corporate Strategy for 2020. The current Corporate Risk Register residual likelihood matrix is attached at Appendix 2.

The main changes to the corporate risk register have been the addition of new risks relating to the delivery of higher apprenticeships, the potential impact of the EU Referendum result, and the organisation of placements activity across the institution.

The principal risks facing the University relate to student recruitment, income generation, the failure to respond effectively to policy change or maintain and enhance the University's reputation and increasing pension deficits / cost of pension provision.

These risks are discussed in more detail in the University's financial statements.

4. Scope and quality of management's ongoing monitoring of risks and the system of internal control

Risk Management is a standing item on every Operations Board agenda, and risk management and internal control are embedded into normal operating routines. Both are subject to regular management review and periodic audit review.

Every Corporate Risk has an Executive Risk Owner. Every member of the Executive is the Risk Champion for their area, and this is embedded into formal letters of delegated authority issued for every financial period.

All matters relating to internal control are reported to Operations Board which also monitors carefully the implementation of agreed recommendations / actions for improvement, as reported through the Internal Audit Progress reports.

5. Results of internal audit work for 2015/16

The University's Internal Auditors for the period under review were PricewaterhouseCoopers LLP (PwC) and their opinion for 2015/16 is set out in their internal audit annual report.

The PwC opinion for 2015/16 is based on their assessment of whether the controls in place support the achievement of management's objectives as set out in their Internal Audit Risk Assessment and Internal Audit Plan 2015/16.

They have completed the program of internal audit work for the financial year ended 31 July 2016, and their opinion is:

Extract from PwC's 2015/16 Internal Audit Annual Report for LSBU

Our opinion is;

“Generally satisfactory, with some improvements required.”

Governance, risk management and control, and value for money arrangements in relation to business critical areas is generally satisfactory. However, there are some areas of weakness in the framework of governance, risk management and control and value for money arrangements which potentially put the achievement of objectives at risk.

Improvements are required in those areas to enhance the adequacy and effectiveness of governance, risk management and control and value for money arrangements.

Basis of opinion

Our opinion is based on:

- All audits undertaken during the year.
- Any follow up action taken in respect of audits from previous periods.
- Any significant recommendations not accepted by management and the resulting risks.
- The effects of any significant changes in the organisation's objectives or systems.

The commentary below provides the context for our opinion and together with the opinion should be read in its entirety.

Commentary

The key factors that contributed to our opinion are summarised as follows:

Our view on London South Bank University's operational control environment and governance arrangements is underpinned by the audit reviews that we have performed during the year. There has been one high risk rated report, two medium risk rated reports and two low risk rated reports prepared during the financial year. The findings from these reports are not considered significant in aggregate to the system of internal control. None of the individual assignments completed in 2015/16 have an overall classification of critical risk.

We note that the strength of control and governance of London South Bank University's IT environment continues to be an area which requires management focus. Our Information Security review has been classified as high risk for 2015/16; this review was also classified as high risk in both our 2013/14 and 2014/15 Annual Opinion. While our risk rating is consistent with prior year, we recognise that a significant amount of work has been done to update and rationalise the IT controls in place and improvements have been made.

In addition to our Information Security report, we performed a specialist review over the external infrastructure. This review identified six recommendations required to mitigate the risk of an external malicious attack. Our work found that London South Bank University is running unsupported and outdated software on services visible over the internet; this exposes the infrastructure to attacks and could potentially compromise those services. We note that management directed us to look at this area because it was a known risk to the organisation and this has helped form our opinion that while these findings are not indicative of systematic threats to the entire control and governance environment, they do suggest that the IT control environment needs to be strengthened.

London South Bank University's risk management arrangements continue to be strong as evidenced by our low risk report on Risk Management. The risk management approach integrates risk management with the strategic and business planning process; this is in line with good practice, as many of the institutions included in our 2016 Risk Management Benchmarking Exercise did not align risks to corporate objectives. This will help to ensure resources are directed at the highest priority risks and are managed efficiently and effectively.

Our Continuous Auditing work shows that on the whole the core financial control environment has remained robust during the year with no significant exceptions or control recommendations raised. Performance has slightly declined towards the end of the year; untimely preparation and authorisation of reconciliations is a recurring theme, affecting Payroll and General Ledger. We have also continued to see exceptions affecting starter and leaver documentation within Payroll, which was either missing or has not been authorised on a timely basis.

The timely implementation of internal audit recommendations by management is a key indicator of good governance and a target rate of 75%+ should be aspired to by management. London South Bank University's implementation rate has improved in 2015/16; 88% of agreed actions have been implemented compared to 78% in the 2014/15.

Our work over value for money indicates that the processes in place to ensure value for money is achieved are in accordance with good practice, for example: adherence to financial controls and use of purchase consortiums.

6. Extent and frequency of communication to the Board (and other committees)

Regular reports on risk and control matters have been presented to the Board and its Committees throughout the year as set out below. These are in addition to the detailed papers at this meeting.

Board of Governors	Report	Purpose
14 th July 2016	Key performance indicators	To note a progress report from the Vice Chancellor
	Corporate risk register	To note a report from the Chief Financial Officer
	HEFCE Annual Mid Year Accountability Return	To approve the return to Hefce including the 5 year forecast.
19 th May 2016	Key Performance Indicators	To consider the Vice Chancellor's report and note developments
	Corporate risk register	To consider a report from the Chief Financial Officer
17 th March 2016	Corporate risk register	To note and update report from the Chief Financial Officer
	Key performance indicators	To consider the Vice Chancellor's report and note developments
26 th November 2015	Corporate risk register	To note and update report from the Chief Financial Officer
	Key performance indicators	To consider the Vice Chancellor's report and note developments
	Annual report from Audit Committee	To note report from the Chair of Audit Committee
	Audit Committee report on the accounts	To note report from the Chair of Audit Committee
	Annual report and	To approve report from the Chief

26 th November 2015	financial statements for year ended 31 July 2015	Financial Officer
	Report from the Finance Planning and Resources Committee on the accounts	To note report from the Chair of Finance Planning and Resources Committee
	External Audit key issues memorandum	To note report from the External Auditors (Grant Thornton)
	HEFCE annual accountability return	To note report from the Chief Financial Officer
21 st October 2015	Corporate risk register	To note detailed annual review from the Chief Financial Officer
	Key performance indicators	To consider the Vice Chancellor's report and note developments
	Corporate Governance Statement	To approve

Audit Committee	Report	Purpose
9 th June 2016	Corporate risk report	To consider the report on corporate risks from the Chief Financial Officer
	Internal Audit progress report 2014/15	To note report from internal auditors on audit progress for 2014/15
	Internal Audit Reports 2014/15:	To note reports completed from 2014/15 internal audit plan
	<ul style="list-style-type: none"> • Continuous Audit into Key Financial Systems – 15/16 period 1 • Continuous Audit into Student Data – 15/16 period 2 • Data Quality Internal Audit Report • Research & Enterprise Contracts Report 	
	Internal Audit plan 2015/16	To preview plan from internal auditors for activity in 2016/16
	External audit plan for 2015/16	To approve plan from external auditors
	Corporate risk report	To consider the report on corporate

11 th February 2016		risks from the Chief Financial Officer
	Internal Audit progress report 2014/15	To note report from internal auditors on audit progress for 2014/15
	Internal Audit Reports 2014/15:	To note reports completed from 2014/15 internal audit plan
	<ul style="list-style-type: none"> • Continuous Audit into Student Data – 15/16 period 1 	
5 th November 2015	Corporate risk report	To consider the report on corporate risks and mitigating actions
	External Reporting (HESES HESA) progress report	To note progress report by Pro-Vice Chancellor (Academic)
	Draft report and accounts for year ended 31 July 2015	To consider the report from the Chief Financial Officer
	Internal audit annual report	To note report from internal auditors
	Internal Audit Reports 2015/16	To note reports completed from 2015/16 internal audit plan
	<ul style="list-style-type: none"> • 	
	Internal audit progress report	To note report from internal auditors on audit progress for 2015/16
	Audit Committee Annual Report	To approve the Audit Committee Annual Report
HEFCE assurance report	To note a report from HEFCE	
24 th September 2015	Corporate risk report	To consider the report on corporate risks and mitigating actions
	Internal Audit progress report 2014/15	To note report from internal auditors on audit progress for 2014/15
	Annual report on effectiveness of internal controls	To consider this report from the Chief Financial Officer
	Internal Audit Reports	To note reports completed as part of the 2014/15 audit plan
	<ul style="list-style-type: none"> • Continuous Audit into Key Financial Systems – 14/15 period 3 • Change Portfolio Transition Review 	

	<ul style="list-style-type: none"> • Risk Management 	
	External Reporting (HESES HESA) progress report	To note progress report by Pro-Vice Chancellor (Academic)

Finance Planning & Resources	Report	Purpose
28 th June 2016	Key performance indicators update	To consider the corporate plan KPIs progress report
5 th May 2016	Key performance indicators update	To consider the corporate plan KPIs progress report
1 st March 2016	Key performance indicators update	To consider the corporate plan KPIs progress report
17 th November 2014	Key performance indicators update	To consider the corporate plan KPIs progress report
22 nd September 2014	Key performance indicators update	To consider the corporate plan KPIs progress report

In addition:

The Audit Committee will have reviewed the following reports at meetings in September 2016 and October 2016 before the accounts are signed:

- The financial statements, including the Statement of Internal Control
- final annual report of the internal auditors for the year ended 31 July 2016
- External auditor's Key Issues memorandum (KIM).

The Board will conduct a detailed review of the corporate risk register at its meeting in October 2016.

7. Incidence of significant control failings or weaknesses during the year

There have been no reportable incidents of significant control failings or weaknesses during the year.

The internal auditors have identified some control design and operating effectiveness issues around data security and these are being addressed.

Regular anti-fraud, bribery and corruption reports have been submitted to each meeting of the Audit Committee.

8. Effectiveness of the University's external reporting processes

No significant issues have arisen as a result of the University's external reporting processes other than matters already covered within the Corporate Risk framework.

DRAFT

APPENDIX 1

Statement on Internal Control

As the governing body of London South Bank University, we have responsibility for ensuring that there is a process for maintaining a sound system of internal control that supports the achievement of policies, aims and objectives of the University, whilst safeguarding the public and other funds and assets for which we are responsible, in accordance with the responsibilities assigned to the governing body in the Memorandum and Articles of Association, and the Memorandum of Assurance and Accountability with HEFCE.

The system of internal control is designed to manage rather than eliminate the risk of failure to achieve policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness.

The system of internal control is based on an ongoing process linked to the achievement of institutional objectives and designed to identify the principal risks to the achievement of policies, aims and objectives, to evaluate the nature and extent of those risks and to manage them efficiently, effectively and economically. This process has been in place for the year ended 31 July 2016 and up to the date of approval of the financial statements, and accords with HEFCE guidance.

As the governing body, we have responsibility for reviewing the effectiveness of the system of internal control. The following processes have been established:

- We meet a minimum of seven times a year (including 2 strategy days) to consider the plans and strategic direction of the institution;
- The approach to internal control is risk based, including a regular evaluation of the likelihood and impact of risks becoming a reality;
- The Audit Committee provide oversight of the risk management process and comments on its effectiveness;
- We receive periodic reports from the chair of the Audit Committee concerning internal control and we require regular reports from managers on internal control activities and the steps they are taking to manage risks in their areas of responsibility, including progress reports on key projects;
- The Audit Committee receives regular quarterly reports from management;
- Internal audit is outsourced to an external provider. The Audit Committee receives regular reports from the internal auditor, which include their independent opinion on the adequacy and effectiveness of the institution's system of internal control, governance and risk management processes, together with recommendations for improvement;
- The internal audit programme has been aligned with the University's corporate risk register;

- An organisation-wide register of key corporate risks is maintained, together with individual risk registers for each school and professional service group. Review procedures cover risk to achievement of strategic objectives, operational business matters, and regulatory compliance as well as financial risk;
- The Operations Board meets regularly to consider risk, assess the current exposure and keep up to date the record of key corporate risks facing the University;
- A network of risk champions exists to support risk management activity in all schools and professional service groups; Update training is provided as required to support delivery;
- Formal risk management and internal control procedures have been embedded within ongoing operations.

Our review of the effectiveness of the system of internal control is informed by internal audit, which operates to standards defined in the HEFCE Audit Code of Practice and which was last reviewed for effectiveness by the HEFCE Audit Service in July 2011. The internal auditors submit regular reports, which include their independent opinion on the adequacy and effectiveness of the institution's system of internal control, governance and risk management processes, with recommendations for improvement.

Our review of the effectiveness of the system of internal control is also informed by the work of the executive managers within the institution, who have responsibility for the development and maintenance of the internal control framework, and by comments made by the external auditors in their management letter and other reports.

APPENDIX 2: Corporate Risk Register: Residual Likelihood Matrix

Date: 12th September 2016 **Author:** John Baker – Corporate & Business Planning Manager **Executive Lead:** Richard Flatman – Chief Financial Officer

Page 280		2: Revenue reduction if marketing and admissions process does not achieve recruitment targets (IM)	1: Lack of capability to respond to policy changes & shifts in competitive landscape (DP)	4 Critical <i>fail to deliver corporate plan / removal of funding or degree awarding status, penalty / closure</i>	Impact
	457: Anticipated international student revenue unrealised (PI)	6: Management Information perceived as unreliable, or doesn't triangulate (RF) 14: Loss of NHS contract income (WT) 305: Data not used / maintained securely (IM) 362: Low staff engagement impacts performance negatively (ME) 3: Increasing pensions deficit (RF) 402: Income growth from R&E unrealised (PI) 467: Progression rates don't rise (PB) 495: Higher Apprenticeship degrees (PB)	37: Affordability of Capital Expenditure investment plans (RF)	3 High <i>significant effect on the ability for the University to meet its objectives and may result in the failure to achieve one or more corporate objectives</i>	
	517: Impact of EU Referendum result on operating conditions & market trends (DP)	398: Academic programmes not engaged with technological and pedagogic developments (SW)	494: Inconsistent delivery of placement activity across the institution (SW)	2 Medium <i>failure to meet operational objectives of the University</i>	
				1 Low <i>little effect on operations</i>	
	3 - High <i>The risk is likely to occur short term</i>	2 - Medium <i>This risk may occur in the medium to long term.</i>	1 - Low <i>This risk is unlikely to occur</i>		
	Residual Likelihood				
Executive Risk Spread: VC – 2, DVC – 2, CFO – 3, PVC-S&E – 2, PVC-R&EE – 2, COO – 2, Dean Health – 1, ExD-HR – 1, US - 0					

	CONFIDENTIAL
Paper title:	Modern Slavery Act – draft statement
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	James Stevenson
Executive sponsor:	James Stevenson
Purpose:	Information
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	N/A
Recommendation:	To recommend the draft statement of approval by the Board of Governors (subject to further review by the time limited working group).

The Executive recommends to Audit Committee a draft statement which complies with the Modern Slavery Act 2015.

The Act requires commercial organisations that supply goods or services (including incorporated educational and charitable organisations), having a global turnover above £36 million, to publish an annual slavery and human trafficking statement.

The statement must:

1. disclose what steps the organisation has taken to ensure that human trafficking is not taking place in any of its supply chains or its business; or state that it has taken no such steps;
2. be signed by a member of the governing body and approved by the board; and
3. be published:
 - for each financial year that ends on or after 31st March 2016 (and annually thereafter);
 - within six months of the organisation's financial year end; and
 - on a prominent place on the company website.

- The draft statement refers to the Ethical Trading Initiative's base code on respect for workers worldwide (code attached for reference)

The time limited working group with representatives from procurement, the schools, HR policy, estates and international is reviewing the detail of the statement. A further meeting will take place shortly to finalise the statement, additional representation from enterprise and ICT will be consulted.

The Audit Committee is requested to:

- recommend the draft statement for approval by the Board of Governors in November 2016 (subject to further review by the time limited working group).

Anti-slavery and Human Trafficking Statement
● **September 2016**

1. Introduction

- 1.1 This statement is made under the Modern Slavery Act 2015 and sets out the steps that London South Bank University (LSBU) is taking to ensure that slavery and human trafficking are not taking place within its supply chain or its business.
- 1.2 LSBU is a UK higher education institution with c.18,000 students and c.1,800 employees. LSBU purchases around £ • m p.a. in goods, services and works through various supply chain arrangements.

2. Policy on slavery and human trafficking

- 2.1 LSBU is committed to procuring goods and services and employing people without causing harm to others. In doing so, LSBU is committed to supporting the UK Government's approach to implementing the UN Guiding Principles on Business and Human Rights.
- 2.2 In implementing this approach LSBU supports the Base Code of the Ethical Trading Initiative. The ETI Base code is founded on the conventions of the International Labour Organisation (ILO) and is an internationally recognised code of labour practice:
- employment is freely chosen
 - freedom of association and the right to collective bargaining are respected
 - working conditions are safe and hygienic
 - child labour shall not be used
 - living wages are paid
 - working hours are not excessive
 - no discrimination is practiced
 - regular employment is provided
 - no harsh or inhumane treatment is allowed

3. Identified risks and mitigation

- 3.1 Direct employment – LSBU mitigates the risk of modern slavery in directly employed staff by following its own policies on selection and recruitment.
- 3.2 Agency staff – agency staff are recruited through established sources, which should provide assurance that they comply with the requirements of legislation relating to the rights and welfare of their candidates and employees.
- 3.3 Students – although the risk is low, LSBU recognises that students living in south London and the surrounding area may become aware of instances of modern slavery or human trafficking. If such circumstances occur, students will be encouraged to seek assistance, support and advice on their wellbeing which can be sourced through the Student Life Centre.
- 3.4 In addition, identification of malpractice within LSBU globally may be referred to the Speak Up helpline, which is an independent reporting line.

4. LSBU's supply chain

4.1 LSBU's supply chain includes the following categories:

- professional services
- ICT equipment and services
- estates goods and services
- laboratory and workshop consumables and equipment

[to verify – LSBU's reasonable assessment at this time is that the principal areas which carry material risks are office supplies, laboratory consumables, ICT and AV equipment, and some estates services, such as cleaning, catering and security services.]

Current action

LSBU's procurement is either: (1) collaborative, through regional HE purchasing consortia; or (2) by in-house tendering and contracting. LSBU engages with its purchasing consortia to support the inclusion of ethical sustainability, including addressing slavery and human trafficking, in their procurement programmes.

LSBU's in-house tendering and contracting processes include some pre-qualification clauses which address the London Living Wage. LSBU's catering, security and reception contracts already include this requirement. LSBU is reviewing its standard terms and conditions in order to cover modern slavery and human trafficking.

[to verify – LSBU uses the DEFRA Prioritisation tool and the Responsible Procurement Code as tools to assess the risks and to monitor progress with mitigation of risk.]

The future

In the medium term, LSBU wishes to better understand its supply chain and to encourage greater transparency and responsibility towards people working within them.

[need to verify – LSBU intends to identify those supply chains which may represent a medium to high risk of modern slavery, human trafficking, forced and bonded labour, and labour rights violations. LSBU will record this assessment of risk using the DEFRA Prioritisation tool and the Responsible Procurement Code, and working with our suppliers will more closely monitor this supply chains that have been identified as a potential risk and take appropriate action as necessary. We envisage identifying such action in collaboration with our purchasing consortium partners and with appropriate NGOs.]

This statement has been approved by LSBU's Board of Governors and will be reviewed annually.

Board of Governors
• October 2016

The ETI Base Code

This document was amended 01 April 2014 with revisions to clause 6, Working hours are not excessive.

1. Employment is freely chosen
 - 1.1 There is no forced, bonded or involuntary prison labour.
 - 1.2 Workers are not required to lodge "deposits" or their identity papers with their employer and are free to leave their employer after reasonable notice.
2. Freedom of association and the right to collective bargaining are respected
 - 2.1 Workers, without distinction, have the right to join or form trade unions of their own choosing and to bargain collectively.
 - 2.2 The employer adopts an open attitude towards the activities of trade unions and their organisational activities.
 - 2.3 Workers representatives are not discriminated against and have access to carry out their representative functions in the workplace.
 - 2.4 Where the right to freedom of association and collective bargaining is restricted under law, the employer facilitates, and does not hinder, the development of parallel means for independent and free association and bargaining.
3. Working conditions are safe and hygienic
 - 3.1 A safe and hygienic working environment shall be provided, bearing in mind the prevailing knowledge of the industry and of any specific hazards. Adequate steps shall be taken to prevent accidents and injury to health arising out of, associated with, or occurring in the course of work, by minimising, so far as is reasonably practicable, the causes of hazards inherent in the working environment.

- 3.2 Workers shall receive regular and recorded health and safety training, and such training shall be repeated for new or reassigned workers.
- 3.3 Access to clean toilet facilities and to potable water, and, if appropriate, sanitary facilities for food storage shall be provided.
- 3.4 Accommodation, where provided, shall be clean, safe, and meet the basic needs of the workers.
- 3.5 The company observing the code shall assign responsibility for health and safety to a senior management representative.

4. Child labour shall not be used

- 4.1 There shall be no new recruitment of child labour.
- 4.2 Companies shall develop or participate in and contribute to policies and programmes which provide for the transition of any child found to be performing child labour to enable her or him to attend and remain in quality education until no longer a child; “child” and “child labour” being defined in the appendices.
- 4.3 Children and young persons under 18 shall not be employed at night or in hazardous conditions.
- 4.4 These policies and procedures shall conform to the provisions of the relevant ILO standards.

5. Living wages are paid

- 5.1 Wages and benefits paid for a standard working week meet, at a minimum, national legal standards or industry benchmark standards, whichever is higher. In any event wages should always be enough to meet basic needs and to provide some discretionary income.
- 5.2 All workers shall be provided with written and understandable information about their employment conditions in respect to wages before they enter employment and about the particulars of their wages for the pay period concerned each time that they are paid.
- 5.3 Deductions from wages as a disciplinary measure shall not be permitted nor shall any deductions from wages not provided for by national law be permitted without the expressed permission of the worker concerned. All disciplinary measures should be recorded.

6. Working hours are not excessive

6.1 Working hours must comply with national laws, collective agreements, and the provisions of 6.2 to 6.6 below, whichever affords the greater protection for workers. Sub-clauses 6.2 to 6.6 are based on international labour standards.

6.2 Working hours, excluding overtime, shall be defined by contract, and shall not exceed 48 hours per week.*

6.3 All overtime shall be voluntary. Overtime shall be used responsibly, taking into account all the following: the extent, frequency and hours worked by individual workers and the workforce as a whole. It shall not be used to replace regular employment. Overtime shall always be compensated at a premium rate, which is recommended to be not less than 125% of the regular rate of pay.

6.4 The total hours worked in any seven day period shall not exceed 60 hours, except where covered by clause 6.5 below.

6.5 Working hours may exceed 60 hours in any seven day period only in exceptional circumstances where all of the following are met:

- this is allowed by national law;
 - this is allowed by a collective agreement freely negotiated with a workers' organisation representing a significant portion of the workforce;
 - appropriate safeguards are taken to protect the workers' health and safety;
- and
- the employer can demonstrate that exceptional circumstances apply such as unexpected production peaks, accidents or emergencies.

6.6 Workers shall be provided with at least one day off in every seven day period or, where allowed by national law, two days off in every 14 day period.

* International standards recommend the progressive reduction of normal hours of work, when appropriate, to 40 hours per week, without any reduction in workers' wages as hours are reduced.

7. No discrimination is practised

7.1 There is no discrimination in hiring, compensation, access to training, promotion, termination or retirement based on race, caste, national origin,

religion, age, disability, gender, marital status, sexual orientation, union membership or political affiliation.

8. Regular employment is provided

- 8.1 To every extent possible work performed must be on the basis of recognised employment relationship established through national law and practice.
- 8.2 Obligations to employees under labour or social security laws and regulations arising from the regular employment relationship shall not be avoided through the use of labour-only contracting, sub- contracting, or home-working arrangements, or through apprenticeship schemes where there is no real intent to impart skills or provide regular employment, nor shall any such obligations be avoided through the excessive use of fixed-term contracts of employment.

9. No harsh or inhumane treatment is allowed

- 9.1 Physical abuse or discipline, the threat of physical abuse, sexual or other harassment and verbal abuse or other forms of intimidation shall be prohibited.

The provisions of this code constitute minimum and not maximum standards, and this code should not be used to prevent companies from exceeding these standards. Companies applying this code are expected to comply with national and other applicable law and, where the provisions of law and this Base Code address the same subject, to apply that provision which affords the greater protection.

Note: We make every effort to ensure that the translations of the ETI Base Code and Principles of Implementation are as complete and accurate as possible. However, please note that in both cases it is the English language documents which should be treated as the official versions.

		CONFIDENTIAL
Paper title:	Corporate Governance statement	
Board/Committee	Audit Committee	
Date of meeting:	22 September 2016	
Author:	Michael Broadway, Deputy University Secretary	
Executive sponsor:	James Stevenson, University Secretary and Clerk to the Board of Governors	
Purpose:	Approval	
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	N/A	
Recommendation:	The meeting is requested to approve the Corporate Governance statement for inclusion in the financial statements.	
Matter previously considered by:	Executive	7 September 2016

Executive Summary

The Corporate Governance Statement is intended to assist readers of the financial statements in obtaining an understanding of the governance and legal structure of the University. It sets out the governance and legal structure of the University and how the Board complies with the Higher Education Code of Governance (CUC, 2014). In line with HEFCE guidance, this is the first year reporting against the 2014 Code.

The committee is requested to approve the draft Corporate Governance Statement for inclusion in the annual report.

Corporate Governance Statement

The following statement is given to assist readers of the financial statements in understanding the governance and legal structure of the University.

The University's Board of Governors is committed to maintaining the highest standards of corporate governance. In carrying out its duties it has regard to:

- The CUC Higher Education Code of Governance
- The UK Corporate Governance Code (where applicable)
- The seven principles of standards in public life
- The HEFCE Memorandum of Assurance and Accountability and the Audit Code of Practice
- The Directors' duties as set out in sections 170 – 177 of the Companies Act 2006
- The Charity Commission's Guidance on Public Benefit and its duties as charity trustees of compliance, prudence and care
- Other legislative requirements of corporate and Higher Education bodies
- The University's Articles of Association and standing orders

Governance and Legal Structure

London South Bank University is a company limited by guarantee and an exempt charity within the meaning of the Charities Act 2011. Its objects and powers are set out in its Articles of Association. The Articles provide the governance framework of the University and set out the key responsibilities of the Board of Governors and its powers to delegate to committees, the Vice Chancellor and the Academic Board.

Compliance with the CUC Higher Education Code of Governance

The Board has complied with all aspects of the Higher Education Code of Governance (CUC, December 2014) during the year under review, as demonstrated below. References to paragraphs of the code are shown in brackets below.

Decision making

London South Bank University is led by a Board of Governors, which is collectively responsible for the strategic direction of the University, approval of major projects and partnerships and ensuring that the potential of every student is maximised (1.1).

The Board has agreed a Schedule of Matters Reserved which establishes the responsibilities of the Board and its committees. The Board, and where appropriate, its committees make decisions by consensus at meetings or electronically (2.4). The schedule is reviewed on an annual basis.

During the year, the Board met five times (five in 2014/15). In addition, the Board held two strategy days (two in 2014/15) allowing further time to discuss and debate longer-term strategic challenges for the University. All governors are expected to attend meetings and to contribute effectively. Attendance at meetings is recorded and monitored by the Chair. In the year under review there was a 93% (2014/15: 90%) attendance rate at Board meetings.

The Board has due regard to Charity Commission guidance on public benefit when making decisions (see separate statement of public benefit on page (•) (1.2.) It receives assurance that the institution meets the requirements of the Memorandum of Assurance and Accountability are followed through the remit of the Audit Committee (1.3).

Compliance

All governors and members of the Executive are required to declare their interests on appointment, on an annual basis and are required to declare any interests which relate to decisions at meetings. During the year under review, all declared interests were authorised by the Board. No conditions were attached to any of these interests (2.2.) The governing body affirms that it makes decisions without any undue pressure from external interest groups, which is assured through the declaration of interests process (2.3.)

The Board receives annual reports on the institution's compliance with key legislation, for example health and safety, equality, diversity and inclusion and otherwise by exception reporting (3.6.) In addition, independent governors have the right to external, independent advice at the University's expense where necessary in order to fulfil their duties. The Board reviews the delegated authority annually which includes a review of the accountable officer's authority. Material adverse change is reported to HEFCE when discovered and annually as part of the Accountability and Assurance statement (3.6.) No material adverse changes were reported to HEFCE during the year.

The Board receives regular reports from the Students' Union in relation to its democratic processes and financial practices (2.5).

Sustainability

The Board is responsible for the sustainability of the institution and approves the annual budget, which is aligned to the five year corporate strategy (3.2). The Board oversees the performance and sustainability of the institution by regularly reviewing Key Performance Indicators, management accounts and five year forecasts (3.3.) Overall financial control is delegated to the Chief Financial Officer, who is a member of the Executive and has regular access to the Vice Chancellor, as and when required.

The Board approved the LSBU Sustainability policy during the year under review, which covers institutional and environmental sustainability in its remit.

Academic governance

The Board has oversight of academic governance across the institution, regularly meeting with the Academic Board to discuss strategy. [The Board has reviewed the quality process and agreed an assurance statement during the year under review – *to confirm at the November board.*] With regard to terms and conditions of academic staff, including pay awards and promotion opportunities, the Board has regard to the need to ensure that academic staff have freedom within the law to question and test received wisdom and to put forward new ideas and controversial or unpopular opinions, without placing themselves in jeopardy of losing their jobs or any privileges they may have at the University (4.1, 4.2, 4.3.)

External activities

The Board reviews all proposals for all significant, external activities and independent legal advice is sought, if necessary. Due diligence is conducted when entering into major projects that have significant risk associated with them (5.1.)

Equality and Diversity

The Board receives an annual report on the institution's compliance with the public sector equality duty under the Equality Act 2010. The Board also receives a progress report against agreed Equality, Diversity and Inclusion action plans at the institution.

The Board regularly reviews its composition and considers equality and diversity in its appointments. An Equality, Diversity and Inclusion plan is being developed for board appointments (6.3, 6.4, 6.5.)

Structures and processes

The Board when fully complemented consists of 18 governors: 13 independent governors (7.1), the Vice Chancellor, two student governors and two academic staff members nominated by the Academic Board. Governors serving for the period are listed on page (•) The Board determines the number and composition of the Board of Governors within parameters set by the University's Articles of Association. Under the Article, the Board has the power to remove any governor from office if they breach their terms of office. (7.2) On appointment, governors also agree to act in accordance with the seven principles of public life and the university values. (1.2, 1.4, 2.1)

Committees

The Board delegates authority to a number of committees. All committees are formally constituted with appropriate terms of reference, which are reviewed annually (3.6.) Terms of reference and membership of each committee are available on the

governance pages of the University's website. Each committee have a majority of independent governors. The chairs of each committee are set out below under Key Individuals.

The following committees met throughout the year:

- Appointments Committee
- Audit Committee
- Finance, Planning and Resources Committee
- Major Projects and Investment Committee
- Nomination Committee (including special meetings to select a Chancellor)
- Remuneration Committee

There is a Nominations committee to recruit new independent governors (7.3). Recommendations are made to the Appointments Committee, which makes the final decision on appointment. A written description of the role and capabilities required of governors has been agreed by the Nomination Committee. Candidates are judged against the capabilities required and the balance of skills and experience currently on the Board. The balance of skills and experience of independent governors is kept continually under review by the Nomination Committee.

The Audit Committee has a majority of independent governors (3.12), including a co-opted external member. The Audit Committee produces an annual report for the Board, following HEFCE requirements (3.4, 3.5.) The Audit Committee reviews the effectiveness of the systems of control in place across the institution. The Audit Committee receives an annual report on the quality of data submitted to external bodies (3.8, 3.10.)

There is a Remuneration Committee which decides the remuneration of members of the Executive, including the Vice Chancellor (3.13.) The committee includes the Chair of the Board and has a majority of independent governors (3.14.) No individual is present for discussions that directly affect them. The committee considers comparison information and use of public funding when deciding remuneration (3.15, 3.16.)

The Board completed an independent external governance review in 2015 [and implemented recommended changes (7.11, 7.12) – *to confirm at October 2016 board meeting.*]

Key Individuals

Position	Name
Chair of the Board of Governors	Jeremy Cope
Vice Chair of the Board of Governors	Andrew Owen

Head of Institution (Vice Chancellor and Chief Executive)	David Phoenix
Chair of Audit Committee	Steve Balmont
Chair of Finance, Planning and Resources Committee	Andrew Owen
Chair of Major Projects and Investment Committee	Douglas Denham St Pinnock
Chair of Nominations Committee	Jeremy Cope
Chair of Appointments Committee	Jeremy Cope
Chair of Remuneration Committee	Mee Ling Ng
University Secretary and Clerk to the Board of Governors	James Stevenson

Key individuals can be contacted through the office of the University Secretary and Clerk to the Board of Governors, Mr James Stevenson, at London South Bank University, 103 Borough Road, London SE1 0AA. Published documents are available on the governance section of the University website.

Statement of Primary Responsibilities of the Board of Governors

1. To approve the educational character, mission and strategic vision of the institution, together with its long-term academic and business plans and key performance indicators, and to ensure that these meet the interests of stakeholders.
2. To delegate authority to the head of the institution, as chief executive, for the academic, corporate, financial, estate, personnel and health and safety management of the institution, and to establish and keep under regular review the policies, procedures and limits within such management functions as shall be undertaken by and under the authority of the head of the institution.
3. To ensure the establishment and monitoring of quality assurance and systems of control and accountability, including financial and operational controls and risk assessment, and procedures for handling internal grievances and for managing conflicts of interest.
4. To ensure that processes are in place to monitor and evaluate the performance and effectiveness of the institution against the plans and approved key performance indicators, which should be, where possible and appropriate, benchmarked against other comparable institutions.
5. To establish processes to monitor and evaluate the performance and effectiveness of the governing body itself, and to carry out such reviews at appropriate intervals.
6. To conduct its business in accordance with best practice in higher education corporate governance and with the principles of public life drawn up by the Committee on Standards in Public Life.
7. To safeguard and promote the good name and values of the institution.
8. To appoint the head of the institution as chief executive, and to put in place suitable arrangements for monitoring his/her performance.
9. To appoint a secretary to the governing body and to ensure that, if the person appointed has managerial responsibilities in the institution, there is an appropriate separation in the lines of accountability.
10. To be the employing authority for all staff in the institution and to be responsible for establishing a human resources strategy.
11. To be the principal financial and business authority of the institution, to ensure that proper books of account are kept, to approve the annual budget and financial statements, and to have overall responsibility for the University's assets, property and estate.

12. To be the institution's legal authority and, as such, to ensure that systems are in place for meeting all the institution's legal obligations, including those arising from contracts and other legal commitments made in the institution's name.
13. To make such provision as it thinks fit for the general welfare of students.
14. To act as trustee for any property, legacy, endowment, bequest or gift in support of the work and welfare of the institution or its students.
15. To ensure that the institution's constitution is followed at all times and that appropriate advice to the Board is available to enable this to happen.

	CONFIDENTIAL
Paper title:	Public Benefit statement
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Megan Evans, Governance Assistant
Executive/Operations sponsor:	James Stevenson
Purpose:	Information
Recommendation:	The meeting is requested to review the draft Public Benefit statement.

Matter previously considered by:	Executive	7 September 2016
----------------------------------	-----------	------------------

Executive summary

The Public Benefit Statement forms a mandatory part of the annual report of charities. The Memorandum of Assurance and Accountability with HEFCE states that the following must be included in the audited financial statements:

- A statement that the charity has had regard to the Commission's guidance on public benefit
- A report on how the HEI has delivered its charitable purposes for the public benefit

The statement sets out the University's charitable objects as found in its Articles of Association and how these objects are applied for the public benefit. It sets out how the University advances education for the public benefit. The University's main beneficiaries are identified as its students but with a wider public benefit of the University's activities mainly through research and community work also recognised.

The committee is requested to approve the draft Public Benefit Statement for inclusion in the annual report.

Public Benefit statement

The University is an exempt charity within the meaning of the Charities Act 2011 and is regulated by HEFCE on behalf of the Charity Commission.

Charity Commission Guidance on Public Benefit

The members of the Board of Governors are the charitable trustees of the University. In undertaking its duties the Board of Governors has regard to the Charity Commission's guidance on public benefit.

Aims (Charitable Objects)

The charitable objects (under s.3 Charities Act 2011) of the University, as set out in its Articles of Association, are to:

- conduct a university for the public benefit for the advancement of education, promotion of research and dissemination of knowledge;
- provide full time and part time courses of higher education at all levels; and
- provide facilities to promote these objects and provide associated support and welfare for students.

The University's objects are applied solely for the public benefit, as follows.

The University advances education for the public benefit by:

- providing learning opportunities for its students in the form of enquiry-based and work-related curriculum including access to lectures, seminars, personal tuition and online resources;
- delivering many courses accredited by recognised professional bodies, both full and part time;
- setting and marking assessments and providing evidence of achievement by the awarding of degrees, diplomas and certificates.

The University promotes research and the dissemination of knowledge by:

- undertaking academic research and publishing the results;
- publishing articles in peer-reviewed journals;
- maintaining an academic library with access for students and academics;

The University provides student support and services for students through:

- Wellbeing services, including support for students with disabilities and mental health issues. This includes a counselling service;
- Student advice and guidance services via a one-stop-shop and student helpdesks across both campuses
- Employability services, supporting students who are working while studying, helping students source work experience and graduate opportunities;
- Money advice, including debt management;
- Specific support services for particular groups of students, including care leavers, carers and pregnant students;
- tutorial guidance, assessment and feedback;
- mentoring and coaching;
- providing student accommodation;
- funding some individual students' education through bursaries and fee waivers; providing funds to London South Bank University Students' Union, enabling social, cultural, sporting and recreational activities and volunteering opportunities for the personal development and employability of its students.

Beneficiaries

In carrying out its objects the University benefits the wider public, through research and knowledge transfer, and through the volunteering activities of students; and benefits its students and future students through teaching and learning activities.

The trustees affirm that the opportunity to benefit is not unreasonably restricted. The benefits of learning at London South Bank University are open to anyone who the University believes has the potential to succeed. Throughout its history LSBU has enabled wider access to education. The University's Strategy, 2015-2020 sets clear targets to focus on three key areas, all directly related to providing public benefit: student success; real world impact; and access to education.

Like other universities LSBU must charge tuition fees. However, maintenance loans are available to home full time undergraduates who have applied for funding via Student Finance England. In addition, the University offers financial assistance in the form of scholarships, bursaries and charitable funds to students in need.

The University's curriculum is firmly rooted in professional courses supported by accreditation from professional, statutory and regulatory bodies that enhance

employability and career success. In 2015, 82% of graduates were in graduate employment and/or further study 6 months after leaving (DLHE survey results 2014 – 15). Around 7,000 LSBU students are sponsored to study by their employers, including NHS funded students.

The University also contributes to the wider public benefit through the publication of research. The University performed well in the Research Excellence Framework 2015, with the majority of its research graded as internationally excellent and recognised internationally.

The University sponsors two schools in the local area: the University Academy of Engineering South Bank which opened in September 2014; and a University Technical College which opened in September 2016. This community engagement aims to develop professional opportunities for students who have the ability to succeed and to enhance student success by preparing them for higher education.

Linked charities

The University has one “linked” exempt charity: the LSBU consolidated charitable fund for the welfare of students. This fund was worth £xxx on 31 July 2016 (2015: £765,659). The funds are managed with the aim of securing capital growth and an annual income. In 2015/16 the income received was £xxx (2014/15: £24,709).

During 2015/16 £xxx was distributed to students in hardship and £xxx as prizes for students.

	CONFIDENTIAL
Paper title:	Speak up report
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Michael Broadway, Deputy University Secretary
Executive sponsor:	James Stevenson, University Secretary and Clerk to the Board of Governors
Purpose:	To update the committee on any speak up matters raised since the last meeting
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	N/A - The speak up policy enables workers and students to report any concerns about malpractice, helping to create an open and ethical culture in the workplace.
Recommendation:	The committee is requested to note the report.

Executive Summary

One speak up matter was raised under the Speak Up policy since the last meeting of the Audit Committee. The matter was reviewed by the Chair. An update will be provided at the meeting.

The speak up reporting line has been launched since the last Audit Committee meeting.

One matter has been raised using the system. On 6 September 2016 an anonymous male called Safecall wishing to report autocratic management. When the call handler explained how the system worked the caller decided to reconsider reporting the matter. He may call again later.

This page is intentionally left blank

	CONFIDENTIAL
	PAPER NO:AC26(16)
Paper title:	Anti-Fraud , bribery and corruption report
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Natalie Ferer
Executive/Operations sponsor:	Richard Flatman – CFO
Purpose:	To review the current Anti-Fraud Policy and Fraud Response Plan.
Which aspect of the Strategy/Corporate Delivery Plan will this help to deliver?	Financial Control and Sustainability.
Recommendation:	That the Committee notes this report

Matter previously considered by:	Audit committee	At each meeting
Further approval required?	n/a	On:

Summary

There are no matters to report for the period under review.

Recommendation

That the Committee notes this report.

This page is intentionally left blank

Paper title:	Committee business plan, 2016/17
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Michael Broadway, Deputy University Secretary
Board sponsor:	Steve Balmont, Chair of the Committee
Purpose:	To inform the committee of its annual business plan
Recommendation:	To approve the committee's annual business plan

Matter previously considered by:	Audit Committee	At each meeting
Further approval required?	No	Date: N/A

Audit Committee Business Plan

The Audit Committee business plan is based on the model work plan for audit committees developed by the CUC. It is intended to help the committee review the adequacy and effectiveness of risk management, control and governance (including ensuring the probity of the financial statements) and for the economy, efficiency and effectiveness of LSBU's activities delegated to it from the Board.

As agreed at the meeting of 5 November 2015, the committee's business plan will be a standing item on agendas.

The plan lists regular items. Ad hoc items will be discussed as required.

The Audit Committee is requested to note its annual business plan.

London South Bank University

	Feb	June	Sept	Nov
Anti-bribery policy review				x
Audit Committee, Annual Report to Board and VC				x
Audit Committee business plan	x	x	x	x
Audit Committee, self-assessment of performance	x			
Membership and Terms of Reference - approve			x	
Speak up report	x	x	x	x
Annual Report and Accounts				x
Anti-fraud policy review		x		
Anti-fraud, bribery and corruption report	x	x	x	x
Data assurance report	x			
Debt write off - annual		x		
External audit findings				x
External audit letter of representation				x
External audit management letter				x
External audit performance against KPI's				x
External audit plan		x		
External audit tender			x	
External auditors - consider policy in relation to non-audit services				x
Financial personnel succession planning	x			

**London South Bank
University**

Internal audit annual report			x (draft)	x (final)
Internal Audit plan - approval		x		
Internal audit plan - review at each audit cttee meeting	x	x	x	x
Internal audit progress reports	x	x	x	x
Internal audit reports (inc continuous audit)	x	x	x	x
Internal Controls - review				x
Pensions assumptions		x (indicative)	x	
Risk Register	x	x	x	x
Risk strategy and appetite			x	
TRAC return to HEFCE to be ratified	x			
TRAC(T) return to HEFCE to be ratified		x		
Value for money report, annual				x

This page is intentionally left blank

Paper title:	Terms of Reference
Board/Committee	Audit Committee
Date of meeting:	22 September 2016
Author:	Michael Broadway, Deputy University Secretary and Clerk to the Board of Governors
Board sponsor:	Steve Balmont, Chair of the Committee
Purpose:	To review the committee's terms of reference
Recommendation:	To note the committee's terms of reference

Executive Summary

The Audit Committee's terms of reference is based on the model terms of reference for audit committees developed by the CUC. It is intended to help the committee review the adequacy and effectiveness of risk management, control and governance (including ensuring the probity of the financial statements) and for the economy, efficiency and effectiveness of LSBU's activities delegated to it from the Board.

The governance effectiveness review took place during 2014/15. Following the review the committee's terms of reference were amended to include the duty to consider significant deviations from business case or concerns following a post investment review. The revised version was approved by the Board on 9 July 2015. No amendments to the current terms of reference are recommended.

The committee's terms of reference and membership are attached for information. The committee is requested to note.

Terms of reference

1. Constitution

- 1.1 The Board of Governors has established a committee of the Board known as the Audit Committee.

2. Membership

- 2.1 The Audit Committee and its chair shall be appointed by the Board, from among its own members, and must consist of members with no executive responsibility for the management of the institution.
- 2.2 There shall be no fewer than three members; a quorum shall be at least two members.
- 2.3 The chair of the Board should not be a member of the committee.
- 2.4 Members should not have significant interests in LSBU.
- 2.5 At least one member should have recent relevant experience in finance, accounting or auditing.
- 2.6 The committee may, if it considers it necessary or desirable, co-opt members with particular expertise.
- 2.7 Members of the committee should not also be members of the finance committee (or equivalent).

3. Attendance at meetings

- 3.1 The chief executive, head of finance (or equivalent), the head of internal audit and a representative of the external auditors shall normally attend meetings where business relevant to them is to be discussed.
- 3.2 At least once a year the committee should meet with the external and internal auditors without any officers present.

4. Frequency of meetings

- 4.1 Meetings shall normally be held four times each financial year. The external auditors or head of internal audit may request a meeting if they consider it necessary.

5. Authority

- 5.1 The committee is authorised by the Board to investigate any activity within its terms of reference. It is authorised to seek any information it requires from any employee, and all employees are directed to co-operate with any request made by the committee.
- 5.2 The committee is authorised by the Board to obtain outside legal or other independent professional advice and to secure the attendance of non-members with relevant experience and expertise if it considers this necessary, normally in consultation with the head of institution and/or chair of the Board. However, it may not incur direct expenditure in this respect in excess of £20,000 without the prior approval of the Board.
- 5.3 The Audit Committee will review the audit aspects of the draft annual financial statements. These aspects will include the external audit opinion, the statement of members' responsibilities, the statement of internal control and any relevant issue raised in the external auditors' management letter. The committee should, where appropriate, confirm with the internal and external auditors that the effectiveness of the internal control system has been reviewed, and comment on this in its annual report to the Board.

6. Secretary

- 6.1 The secretary to the Audit Committee will be the Clerk to the Board or other appropriate person nominated by the Clerk.

7. Duties

- 7.1 The duties of the committee shall be to:
- 7.1.1 advise the Board on the appointment of the external auditors, the audit fee, the provision of any non-audit services by the external auditors, and any questions of resignation or dismissal of the external auditors;
 - 7.1.2 discuss with the external auditors, before the audit begins, the nature and scope of the audit;
 - 7.1.3 as necessary, to hold regular discussions with the external auditors (in the absence of management where necessary);

- 7.1.4 consider and advise the Board on the appointment and terms of engagement of the internal audit service (and the head of internal audit if applicable), the audit fee, the provision of any non-audit services by the internal auditors, and any questions of resignation or dismissal of the internal auditors;
- 7.1.5 review the internal auditors' audit risk assessment, strategy and programme; consider major findings of internal audit investigations and management's response; and promote co-ordination between the internal and external auditors. The committee will monitor that the resources made available for internal audit by the executive are sufficient to meet LSBU's needs (or make a recommendation to the Board as appropriate);
- 7.1.6 keep under review the effectiveness of the risk management, control and governance arrangements, and in particular review the external auditors' management letter, the internal auditors' annual report, and management responses;
- 7.1.7 monitor the implementation of agreed audit-based recommendations, from whatever source;
- 7.1.8 monitor the proper investigation by the executive of all significant losses and that the internal and external auditors, and where appropriate the funding council's accounting officer, have been informed;
- 7.1.9 oversee the policy on anti-fraud and irregularity, including being notified of any action taken under that policy;
- 7.1.10 satisfy itself that suitable arrangements are in place to promote economy, efficiency and effectiveness;
- 7.1.11 receive any relevant reports from the National Audit Office (NAO), the funding councils and other organisations;
- 7.1.12 monitor annually the performance and effectiveness of the external and internal auditors, including any matters affecting their objectivity, and make recommendations to the Board concerning their reappointment, where appropriate;
- 7.1.13 consider elements of the annual financial statements in the presence of the external auditors, including the auditors' formal opinion, the statement of members' responsibilities and the statement of internal control, in accordance with the funding councils' accounts directions;

- 7.1.14 in the event of the merger or dissolution of the institution, ensure that the necessary actions are completed, including arranging for a final set of financial statements to be completed and signed;
- 7.1.15 advise the Board of Governors on the effectiveness of the internal control system and recommend changes as necessary;
- 7.1.16 review regularly the financial regulations for the supervision and control of financial procedures, accounts, income and expenditure of LSBU and to advise the Board of Governors as necessary;
- 7.1.17 monitor compliance with relevant regulatory and legal requirements (e.g. HEFCE financial memorandum) and report to the Board of Governors as necessary;
- 7.1.18 receive reports made under the “speak up” policy and to monitor annually the performance and effectiveness of the “speak up” policy and procedures;
- 7.1.19 to authorise debt write offs above £50,000. To receive a report on any debt written off below this threshold and approved by the Chief Financial Officer.
- 7.1.20 to consider significant deviations from business case or concerns following a post investment review

8. Reporting procedures

- 8.1 The minutes (or a report) of meetings of the Audit Committee will be circulated to all members of the Board.
- 8.2 The committee will prepare an annual report covering the institution’s financial year and any significant issues up to the date of preparing the report. The report will be addressed to the Board and Vice Chancellor/Chief Executive, and will summarise the activity for the year. It will give the committee’s opinion of the adequacy and effectiveness of the institution’s arrangements for the following:
- risk management, control and governance (the risk management element includes the accuracy of the statement of internal control included with the annual statement of accounts); and
 - economy, efficiency and effectiveness (value for money).
 - management and quality assurance of data submitted to HESA and to HEFCE and other funding bodies

This opinion should be based on the information presented to the committee.
The Audit Committee annual report should normally be submitted to the Board before the members' responsibility statement in the annual financial statements is signed.

Approved by the Board of Governors on 9 July 2015

Membership 2016/17

Chairman

Steve Balmont (Chair)

Independent governor members:

Mee Ling Ng

Shachi Patel

Independent co-opted member:

Roy Waight

In attendance:

External auditors Grant Thornton

Internal auditors PricewaterhouseCoopers