

Meeting of the Audit Committee

4.00* - 6.00 pm on Thursday, 8 February 2018
in 1B16 - Technopark, SE1 6LN

* Pre meeting with the Internal Auditors and the External Auditors at 3.30pm in 1B16, Technopark

Agenda

<i>No.</i>	<i>Item</i>	<i>Pages</i>	<i>Presenter</i>
1.	Welcome and apologies		SB
2.	Declarations of interest		SB
3.	Minutes of the previous meeting	3 - 8	SB
4.	Matters arising	9 - 10	SB
	Internal audit		
5.	Progress report (to discuss)	11 - 34	JM
6.	Fire Safety report (to discuss)	35 - 56	ME
7.	Student Data report (to discuss)	57 - 90	RF
8.	Key Financial Systems report (to discuss)	91 - 146	RF
9.	ICT risk diagnostic report	147 - 180	DM
	Risk and control		
10.	Corporate risk register (to discuss)	181 - 204	RF
	External audit		
11.	Progress report	205 - 210	FN
	Other matters		
12.	South Bank Academies Audit report (to note)	211 - 242	RF
13.	UKVI audits report (to note)	243 - 252	ME
14.	CLA audit report (to note)	253 - 260	JS
15.	Anti-fraud, bribery and corruption report (to note)	261 - 272	RF, CG
16.	Speak up report (to note)	273 - 274	JS

<i>No.</i>	<i>Item</i>	<i>Pages</i>	<i>Presenter</i>
17.	Data assurance report (to note)	275 - 280	RF
18.	GDPR update (to note)	281 - 324	JS
19.	Annual efficiency return (to ratify)	325 - 340	RF
20.	Finance and Management Information (FMI) structure and leadership team (to note)	341 - 342	RF
21.	Prevent and LSBU employee update	343 - 344	IM
22.	TRAC return to HEFCE (to ratify)	345 - 360	RF
23.	Audit Committee business plan (to note)	361 - 368	JK
24.	Matters to report to the Board following the meeting		JK
25.	Any other business		SB

**Date of next meeting
4.00 pm on Thursday, 7 June 2018**

Members: Steve Balmont (Chair), Shachi Blakemore, Duncan Brown and Mee Ling Ng

In attendance: David Phoenix, Natalie Ferer, Richard Flatman, James Stevenson, Joe Kelly, David Mead (for item 9), Craig Girvan (for item 15) and Mandy Eddolls (items 6 and 13)

Internal auditors: Justin Martin, Lucy Gresswell

External auditors: Fleur Nieboer, Jack Stapleton

**Minutes of the meeting of the Audit Committee
held at 4.00 pm on Thursday, 9 November 2017
1B16 - Technopark, SE1 6LN**

Present

Steve Balmont (Chair)
Shachi Blakemore
Duncan Brown
Roy Waight

Apologies

Mee Ling Ng

In attendance

David Phoenix
Mandy Eddolls
Natalie Ferer
Richard Flatman
Ed Spacey
James Stevenson
Shân Wareing
Michael Broadway
Justin Martin
Lucy Gresswell
Fleur Nieboer
Jack Stapleton
Alexandra Barrington

1. Welcome and apologies

The Chair welcomed members to the meeting.

The above apologies had been received.

2. Declarations of interest

No interests were declared on any item on the agenda.

3. Minutes of the previous meeting

The committee approved the minutes of the meeting of 3 October 2017, subject to an amendment to minute 8 and their publication with the proposed redactions.

4. Matters arising

The Executive Director of Organisational Development & HR updated the committee on how the decline in continuous audit performance in payroll is being addressed (minute 8 of 3 October 2017 refers). Payroll processes are

being updated in line with the new HR i-trent system and use of manual workarounds is being eliminated. The committee expected to see progress in payroll as part of the next finance continuous audit report.

The Executive Director of Organisational Development & HR updated the committee on gender pay gap reporting. The gender pay gap at LSBU was below the sector average at 5% and raised no concerns.

The Chief Financial Officer reported that the member of procurement staff was due to attend a disciplinary hearing (minute 8 of 3 October 2017 refers).

Mandy Eddolls left the meeting

5. Final internal audit annual report

The committee noted the final internal audit annual report which had been discussed in detail at its meeting of 3 October 2017. The internal auditor's opinion was unchanged.

6. Internal audit progress report

The committee noted the internal audit progress report for 2017/18. The audit of health and safety had been completed and the report is being finalised.

7. IT risk diagnostic update

The committee noted the update on the IT risk diagnostic audit done by PwC. The report and the management response would come to the audit committee meeting of 8 February 2018.

8. Prevent annual return

Ed Spacey joined the meeting

The committee recommended the Prevent annual report including the HEFCE required statement of assurance to the Board for approval.

Ed Spacey left the meeting

9. GDPR update

The committee noted the update on compliance with the general data protection regulations (GDPR). The Executive will review a costed project plan to mitigate the risk of non-compliance with GDPR. An update would be provided to the next committee meeting.

10. **Annual value for money report**

The committee noted the update on the annual value for money report. Due to changes in HEFCE requirements the annual value for money report would be prepared with the new annual efficiency return to HEFCE in January 2018. The committee requested that the efficiency return is circulated to the committee ahead of submission to HEFCE.

11. **Modern slavery act statement**

The committee approved the current modern slavery act statement for 2016/17 on behalf of the Board, with no changes.

12. **Anti-fraud, bribery and corruption report**

The committee noted the report. One issue of suspected fraud had arisen since the last Audit Committee meeting. The committee noted that the suspected fraud was likely to be the result of a phishing scam. The amount of the fraud was below the threshold for reporting to HEFCE.

It was noted that the suspected fraud was not due to a breakdown in control or lack of compliance in payroll. However, controls in payroll had been strengthened as a result.

13. **Speak up report**

The committee noted the Speak Up report. One new issue had been anonymously raised since the last meeting concerning alleged bullying and harassment in one of the schools. Further detail would be requested from the complainant via the Safecall reporting system. The committee would be kept updated.

14. **Audit Committee business plan**

The committee noted its business plan. The committee noted that, as previously agreed, it would not review the corporate risk register at this meeting.

15. **External Audit progress report**

The committee noted the external auditor's progress report. This was KPMG's first year end audit following appointment as external auditor in April 2017.

The committee noted that the Chief Financial Officer would review the implications of the final HMRC guidance on corporate criminal offences as set out in the Criminal Finances Bill 2017.

16. External audit findings

The external audit partner of KPMG, presented the audit findings for the year ended 31 July 2017. It was reported that the audit was substantially complete pending the finalisation of a few outstanding items. No misstatements or material weaknesses had been identified.

The external audit partner confirmed KPMG's independence from LSBU.

Responding to a query, the Financial Controller confirmed staff are being trained on the management of journals.

The final external audit report would be available for the Board meeting of 23 November 2017.

17. Going concern review

The committee approved the going concern review and recommended that the Board approves the group accounts (which are prepared on a going concern basis). The review provided assurance for the going concern statement in the annual report and accounts.

18. External audit letter of representation

The committee discussed the letter of representation to the auditors, which was recommended to the committee by the executive. The committee noted that the letter contained standard representations only and that no items had been inserted specific to LSBU or as a result of any matters arising during the course of the audit. The committee recommended the letter to the Board for approval.

19. Draft report and accounts for year to 31 July 2017

The committee reviewed the draft report and accounts for 2016/17. The draft surplus was £1.8m.

The committee noted that, on appointment KPMG had received assurance from the previous external auditor, Grant Thornton, that there were no matters to draw to the attention of the Board. Whether to include this assurance in the accounts would be reviewed.

Note 8B on the remuneration policy for senior employees had been expanded for this year.

The committee recommended the accounts to the Board for approval, subject to minor amendments while the audit was being completed.

20. **Audit Committee Annual Report**

The committee approved the draft audit committee annual report to the Board, as recommended by the executive, subject to updating some sections. The final report, when signed by the Chair of the Audit Committee would be submitted to HEFCE.

21. **Annual Provider Review to HEFCE (quality assurance)**

Shân Wareing joined the meeting

The committee discussed the quality assurance return to HEFCE in detail. The committee noted that under HEFCE requirements the Board is required to sign an annual statement to confirm that the Board is assured that LSBU is maintaining its responsibility for improving student academic experience and student outcomes, and that academic standards are set and appropriately maintained.

The committee noted that aspects of quality assurance are regularly reported to the Board through the Vice Chancellor's report, Key Performance Indicators report and the corporate strategy progress report.

The committee noted how LSBU's quality processes were mapped to international quality expectations. The committee noted the action plan for continuous improvement of the student academic experience.

Following the review by the Academic Board and the committee's review of the supporting documentation, the committee recommended the full assurance statement to the Board for approval.

Shân Wareing left the meeting

22. **External audit performance against KPI's**

The committee noted that KPMG, the external auditors, had met or mostly met their agreed key performance indicators and there were no concerns during the course of the audit. The final report would be circulated to the committee for information.

23. External audit - review of non-audit services

The committee noted that during the year 2016/17, KPMG had provided advice in relation to tax computation services.

24. Matters to report to the Board following the meeting

The committee noted that the annual report and accounts, the going concern statement, letter of representation to the auditors, the audit committee annual report and the review of internal controls would be reported to the Board meeting of 23 November 2017.

**Date of next meeting
4.00 pm, on Thursday, 8 February 2018**

Confirmed as a true record

..... (Chair)

**AUDIT COMMITTEE - THURSDAY, 9 NOVEMBER 2017
ACTION SHEET**

Agenda No	Agenda/Decision Item	Action	Officer	Action Status
7.	IT risk diagnostic update	ICT risk diagnostic audit report and management response to February 2018 audit committee meeting	Ian Mehrrens	On agenda
9.	GDPR update	Update to February 2018 audit committee meeting on GDPR	James Stevenson	On agenda
10.	Annual value for money report	Circulate annual efficiency return to committee before submission to HEFCE	Richard Flatman	Circulated to Chair (25.01.18)
15.	External Audit progress report	Update on HMRC Tackling Tax Evasion – corporate offences	Richard Flatman	Verbal update
16.	External Audit findings	Staff training re journal management	Natalie Ferer	Verbal update
22.	External audit performance against KPI's	Circulate final KPI performance report to committee	Natalie Ferer	Completed (By email 15.11.17)
23.	External audit - review of non-audit services	Circulate final non-audit services report to committee	Natalie Ferer	Completed (By email 16.11.17)

This page is intentionally left blank

CONFIDENTIAL	
Paper title:	Internal Audit Progress Report – February 2018
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	For Information; to provide Committee with the current progress of the work of the Internal Audit programme.
Which aspect of the Corporate Strategy will this help to deliver?	The internal audit plan relates to controls and processes that relate to the entire organisation, and provides 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

Executive Summary

61% of the agreed internal audit programme for 17/18 is now complete.

The progress overview accompanies Continuous Audit reports into Student Data and Key Financial Systems, a report into Fire Safety Management, and the report on the ICT Risk Diagnostic surveys and the related action plan..

Seven recommendations were followed up in this period, and two have been implemented (29%), with 1 partially implemented, and 3 allocated a revised due date. (*details in appendix A on p16*)

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

This page is intentionally left blank

Internal Audit Progress Report 2017/18

*London South Bank
University*

FINAL

February 2018

Page 13

Click to launch

Contents

Summary

1 

Activity in the period

2 

Progress against plan

3 

Page 14

Appendices

- A. Follow up on audit actions
- B. Thought leadership



Summary (1 of 2)



Purpose of this report

We are committed to keeping the Audit Committee up to date with Internal Audit progress and activity throughout the year. This summary has been prepared to update you on our activity since the last meeting of the Audit Committee and to bring to your attention any other matters that are relevant to your responsibilities.

Progress against the 2017/18 internal audit plan

We have completed 61% of our 2017/18 internal audit programme for the year. For this Audit Committee, we present the following final reports:

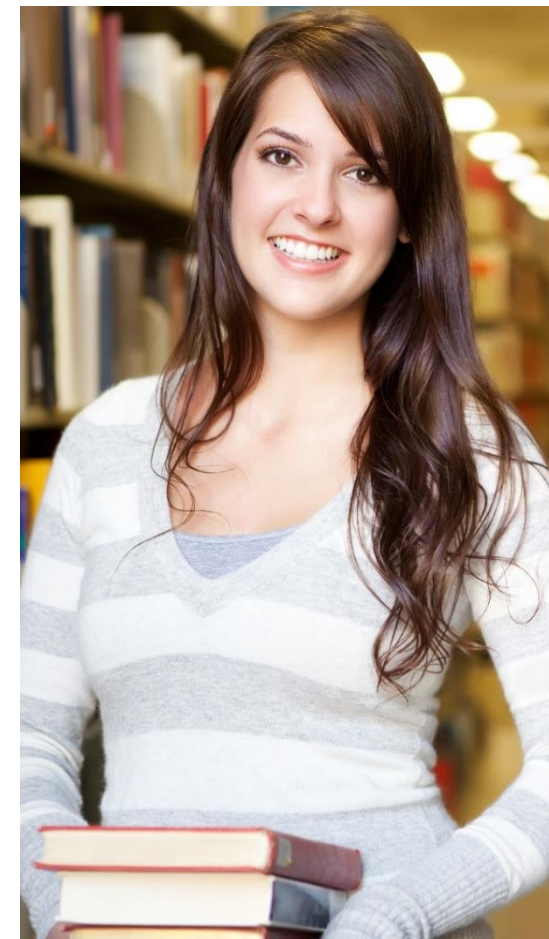
- IT Risk Diagnostic (2016/17);
- Fire Safety Management (Health and Safety);
- Continuous Auditing: Student Data Period 1 – 2017/18; and
- Continuous Auditing: Key Financial Systems Period 2 – 2017/18.

Findings of our Follow Up Work

We have undertaken follow up work on actions with an implementation date of 31/01/2018 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 seven actions have been followed up this quarter:

- Two actions have been implemented (29%) and one action has been closed (14%) as management have implemented changes which supersede our recommendation;
- One action is partially implemented (14%); and
- Three actions have not been implemented (43%) and a new due by date has been agreed.



Summary (2 of 2)



Other Matters

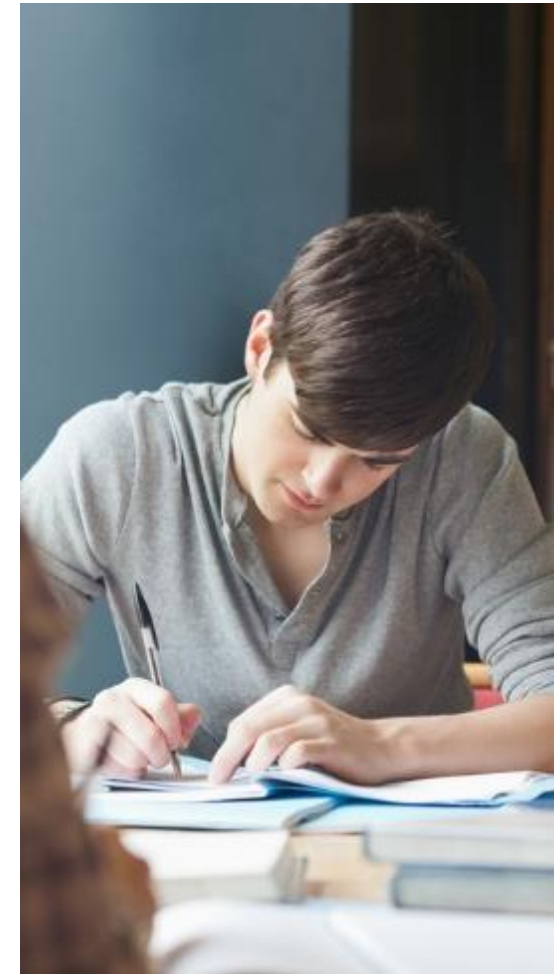
In response to the payroll fraud in September 2017, management requested support from our cyber and fraud experts to assess the internal investigation. We have prepared a letter summarising management's response to the fraud and outlined recommended actions which could be taken to reduce LSBU's exposure to further fraudulent activity.

We were due to report on the International Partnership Arrangements review during this Audit Committee, however due to the breadth of LSBU staff members involved in this review, we are still completing our fieldwork. This report will be presented to the next Audit Committee meeting.

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. In Appendix B we have summarised some of our recent publications.

Recommendations

- That the Audit Committee **notes** the progress made against our 2017/18 Internal Audit Programme.
- That the Audit Committee **comments** on our final report for: IT Risk Diagnostic, Fire Safety Management (Health and Safety), Continuous Auditing: Student Data Period 1 – 2017/18 and Continuous Auditing: Key Financial Systems Period 2 – 2017/18



Activity in the period (1 of 7)



Final reports issued since the previous meeting

IT Risk Diagnostic

The purpose of this review was to establish a baseline understanding of the IT risk environment and maturity of internal controls across the IT Audit landscape within London South Bank University. This was performed by carrying out a series of meetings and workshops with the IT management team, to understand the processes and controls in place across seven core IT areas. Management’s subsequent self-assessment of controls maturity in the seven areas have been benchmarked against both “good practice” and a group of 30+ organisations which includes both public and private sector organisations.

The review presents a view of the maturity of controls in the following seven areas within the IT Audit landscape:

- IT Strategy;
- IT Governance;
- IT Management;
- System Quality;
- System Support & Change;
- IT Operations; and
- Information Security.

London South Bank University has a generally controlled IT function. Our benchmarking exercise has identified that the University has benchmarked typically in the third quartile against peer and similar sized organisations.

This has not been due to widespread absence of an IT control framework however and no single domain was found to be totally lacking in expected controls. The key theme that came out of the review was that efforts need to be made to formalise and update existing controls so that either their scope widens or they become more consistently executed. For example, periodic asset management checks are taken, but not in the context of an actual asset management policy driving ongoing behaviours.

We noted that IT are developing a number of initiatives to rectify certain areas of deficiency. For instance, the University have plans in place to increase their maturity in mapping interdependencies across IT systems and processes and have recently worked to improve training programmes for staff.

The primary objective of the review was to benchmark the IT control environment against peer organisations. As a result of this benchmarking exercise there is also an opportunity to highlight a number of areas that would benefit from review by internal audit in the short, medium and longer term. The key weaknesses areas, each considered as high risk, are as follows:

Activity in the period (2 of 7)



1. IT Governance

Although the University have a formalised IT Security policy in place, there are a number of other IT policies that have not been reviewed and updated. Additionally, the University does not have an up-to-date central repository where all IT policies are stored and periodically reviewed.

There are no IT service level agreements (SLAs) in place between IT and the wider University, as a result there is an absence of effective monitoring of the service provided by IT to ensure it is delivering value for money and supporting the University and its students.

2. Systems Support and Change

There are support teams in place for key components and systems however, there remains some single points of failure (key staff). Additionally, despite the launch of a training database, IT training is informal and infrequent. This may lead to loss or unavailability of knowledge and may result in IT's inability to effectively support the business.

The University have high level and low level designs in place for a number of key systems, however these have not been signed off and are now out of date. Without appropriate and up-to-date documentation in place system performance may degrade due to unrecorded and understood customisation that cannot be rolled back.

It was identified that for some systems all developers retain production access. The absence of access control mechanisms or access reviews around developer access to the production environment may lead to unapproved changes being implemented. This may result in systems instability and significant business disruption.

3. IT Operations

The University have large amounts of legacy hardware in place now unsupported by the vendor or requiring specialist (and expensive) knowledge to maintain and run. This increases the risk that, in the event of an incident, the University will be unable to provide effective support which may result in business disruption.

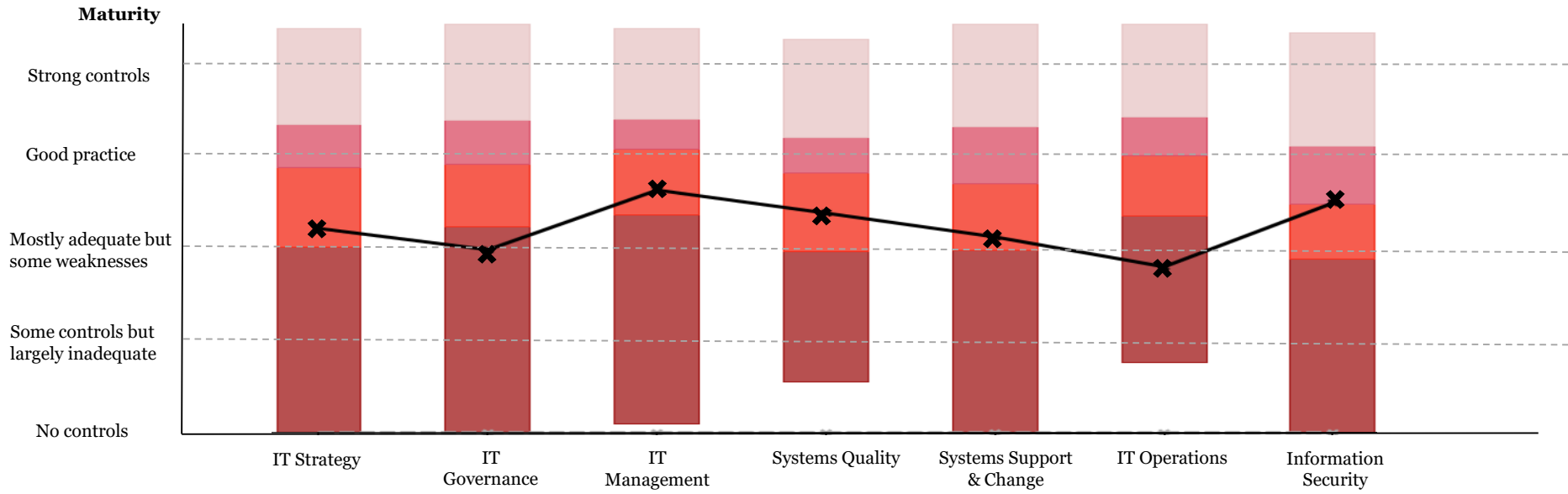
There are no formalised problem management and IT Business Continuity procedures in place. Additionally, the major incident management policy is not aligned to the University's Emergency Management Policy. The absence of formalised and effectively aligned policies may result in an inability to address business needs in case of a major outage.

There are disaster recovery (DR) arrangements in place for specific systems. However, DR plans have not been signed off by appropriate parties. The lack of appropriate IT DR testing may lead to an inability to restore services when needed, resulting in major outages or business disruption.

Activity in the period (3 of 7)



The graph below summarises IT Management’s self assessment of controls maturity across the seven areas of the IT Risk Diagnostic Review.



Average controls maturity

- ✘ Organisation Average Maturity
- Top quartile: Top 25% of the peer group
- Second quartile: Second 25% of the peer group
- Third quartile: Third 25% of the peer group
- Bottom quartile: Bottom 25% of the peer group

Activity in the period (4 of 7)



The table below sets out a summary of areas that may benefit from audit focus in 2017/18 and beyond. The proposed areas of audit focus are grouped by risk level with a short definition being given for each level.

High

Immediate action is recommended to address significant weaknesses in the system of internal controls which exposes the organisation to an unacceptable risk.

Should be considered included as part of FY 17/18 IT Audit plan.

Areas to be considered

- IT Governance (IT Governance)
- Standardisation of IT/ Enterprise Architecture (Strategic Decision Making)
- IT Disaster Recovery (IT Operations)

Medium

Action is recommended within agreed timescales, to address weaknesses in the system of internal control which increases organisational risk.

Should be included as part of IT Audit plan in the next 2 to 3 years.

Areas to be considered

- IT Performance Management (IT Governance)
- Information Classification (Information Security)
- IT Knowledge Management (IT Systems support)

Low

Action should be considered, although the current exposure to risk is unlikely to be significant. Action to be taken is at the discretion of the organisation.

Should be considered its inclusion as part of IT Audit plan in the next 3 to 5 years.

Areas to be considered

- Third Party Management (IT Management)

Activity in the period (5 of 7)



Final reports issued since the previous meeting (continued)

Fire Safety Management – Medium Risk

London South Bank University (LSBU) is planning to release a new fire safety policy. The objective of this audit was to review the processes and controls in place to manage compliance with legislative and regulatory requirements associated with the management of fire related safety risks. The review also explored behaviours and cultures around fire safety.

Key findings:

- It is understood from discussions with the security and safety managers that some occupants of buildings are not responding promptly to fire alarms. This is due to a lack of awareness of how quickly fires can spread, in certain pockets around the organisation;
- There is currently no mechanism (such as an action tracker) in place for checking that deficiencies identified as a result of fire risk assessments are being resolved; and
- Emergency plans do not currently contain information regarding what chemical and/or flammable hazards exist within LSBU buildings and where these are located. We understand that a chemical hazards list has been made available to the emergency services but the security and estates teams were not aware of this.

Good practice noted

- Following the Grenfell tower incident, LSBU employed an external company to undertake an independent review of a number of its buildings to evaluate if there was any significant impact following the Grenfell Tower (fatal fire), London, June 2017.
- The Health Safety and Resilience (HSR) team have a proactive and positive relationship with the emergency services, including sitting on the Southwark emergency planning forum.

Activity in the period (6 of 7)



Final reports issued since the previous meeting (continued)

Continuous Auditing: Student Data Period 1 – 2017/18

Performance in the current period is consistent with previous period: 41 operating effectiveness exceptions were identified in both Period 1 2017/18 and Period 2 2016/17. The testing results suggest that there has been a decline in performance for S2 (Tier 4 controls). The performance for the majority of other control areas has improved. One control design exception were also identified in Period 1 2017/18 (Period 2 2016/17: 1 exception).

Control	P1 17/18 Effectiveness	P1 17/18 Control design	P2 16/17 Effectiveness	P2 16/17 Control design	Trend
S1	11	-	14	-	↑
S2	16	1	-	-	↓
S3	4	-	1	-	↓
S4	-	-	1	-	↑
S5	2	-	6	-	↑
S6	3	-	5	-	↑
S7	1	-	-	1	↓
S8	4	-	8	-	↑
S9	-	-	1	-	↑
S10	-	-	5	-	↑
Total	41	1	41	1	↔

System Classification

Medium Risk



Activity in the period (7 of 7)



Final reports issued since the previous meeting (continued)

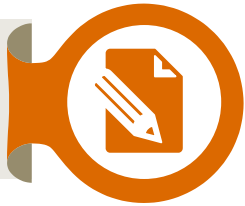
Continuous Auditing: Key Financial Systems Period 2 – 2017/18

Overall, we are pleased to report that there has been an improvement in the performance of key financial systems in the current period. We have seen a marked improvement in the performance of payroll with fewer exceptions identified across all HR and payroll controls compared to the previous period. The performance of Accounts Payable has also improved with fewer exceptions in the current period. We have moved the risk rating of Accounts Receivable to amber as we identified a number of instances where debts were not chased in accordance with the debt recovery policy. The performance of Cash and General Ledger remains green. Our ratings are based on the number and severity of findings noted for controls tested as part of the programme.

The below summary does not include control design issues which are individually risk rated. We identified seven control design findings – one finding was rated high risk, three findings were rated medium risk and three findings were rated low risk.

System / Rating	P2 2017/18	P1 2017/18	P2 2016/17	P1 2016/17	P2 2015/16	P1 2015/16	Trend
Payroll	Green	Red	Amber	Amber	Amber	Green	
Accounts Payable	Green	Amber	Amber	Green	Green	Green	
Accounts Receivable	Amber	Green	Green	Green	Green	Green	
Cash	Green	Green	Green	Amber	Green	Green	
General Ledger	Green	Green	Green	Amber	Green	Green	

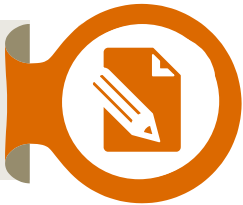
Progress against 2017/18 plan (1 of 3)



The below table outlines the progress against the 2017/18 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 2017 – October 2017											
Continuous Auditing: Key Financial Systems – January 2017 to July 2017											
15 (15)	02/08/2017	14/08/2017	15/09/2017	19/09/2017							
Health and Safety											
12 (12)	18/09/2017	09/10/2017	08/11/2017	26/01/2018	Medium	3	-	-	2	1	-
Quarter 2: November 2017 – January 2018											
International Partnership Arrangements											
10 (8)	29/11/2017	04/12/2017									
Continuous Auditing: Student Data – April 2017 to October 2017											
13 (13)	29/11/2017	04/12/2017	14/12/2017	31/01/2018							

Progress against 2017/18 plan (2 of 3)



Days	ToR	Field work start	Exit Meeting	Final Report	Report Classification	Total findings	Ratings				
							Critical	High	Medium	Low	Advisory
Quarter 3: February 2018 – April 2018											
Continuous Auditing: Key Financial Systems - August 2017 to December 2017											
15 (15)	11/12/2017	08/01/2018	19/01/2018	31/01/2018	N/A						
Continuous Auditing : Student Data - November 2017 to March 2018											
12 (0)					N/A						
HR audit											
10 (0)											
IT audit											
15 (0)											

Progress against 2017/18 plan (3 of 3)



Days	ToR	Field work start	Exit Meeting	Final Report	Report Classification	Total findings	Ratings				
							Critical	High	Medium	Low	Advisory
Quarter 4: May 2017 – July 2017											
Risk Management											
5 (0)											
Other											
18 (13)	Planning, contract management, reporting, value for money and follow up										
Total	125 (76)										

Appendices

Appendix A: Follow up (1 of 4)

Implemented

#	Review	Agreed Action	Original due date	Risk rating	Status
1	Prevent Duties	<p><u>Retention of affiliated events</u></p> <p>We will prepare a centralised listing of LSBU affiliated events taking place both on and off campus.</p>	30/11/2017	<p>●</p> <p>Medium</p>	<p>Implemented</p> <p>All agreed actions have been implemented.</p>
	Placements	<p><u>InPlace</u></p> <p>We will involve key users in the tailoring of the software in terms of reports and monitoring functionality, to enable a smoother transition when the system goes live, and enable the system to be used to the best of it's capacity.</p> <p>We will formulate a general survey which will be input into InPlace and allow wide-scale student interaction and feedback.</p> <p>We will explore the reporting tools within InPlace and utilise a report which will show when placements are coming to an end, so that the placement provider can be contacted to understand their business needs and the possibility of further placements for LSBU students.</p> <p>We will tailor training courses to different schools and user groups to ensure that they understand how to get the best out of the software and how it can improve both staff productivity and student experience.</p> <p>We will use the reporting function on InPlace to track the progress of placement applications and follow-up on slow-moving placement applications where appropriate.</p> <p>Appropriate due diligence checks will be completed before giving placement providers access.</p> <p>If access is granted to placement providers, their access will be limited to prevent them viewing sensitive data.</p>	31/12/2017	<p>●</p> <p>Medium</p>	<p>Implemented</p> <p>All agreed actions have been implemented.</p>

Appendix A: Follow up (2 of 4)

Closed

#	Review	Agreed Action	Original due date	Risk rating	Status
1	Management Information - Data Quality	<p><u>Accuracy of Management Information</u></p> <p><u>Appraisal Completion %</u></p> <p>We will agree the parameters for the Appraisal Completion % to allow reporting on the KPI.</p> <p><u>Teaching Room Utilisation Rate</u></p> <p>The teaching room utilisation KPI reported for 2014/15 will be updated for the November 2014 survey.</p> <p>Prior to the next annual survey (for the 2016/17 financial year), we will confirm the timings of reading weeks to ensure there is a consistent measurement basis.</p> <p><u>Graduate Level Employment</u></p> <p>We will investigate and correct the course mapping to capture all applicable students in the KPI.</p>	31/12/2017	<p>●</p> <p>Medium</p>	<p>Closed</p> <p>A new reporting and visualisation tool has been implemented, meaning this agreed action has been superseded.</p>

Appendix A: Follow up (3 of 4)

Partially Implemented

#	Review	Agreed Action	Original due date	Risk rating	Status
4	Data Security	<p>Security</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	31/12/2017	<p>●</p> <p>High</p>	<p>Partially implemented</p> <p>We are not yet tracking MAC OSX in SCCM nor have we made the changes to the password policy. All other agreed actions have been implemented.</p>

Appendix A: Follow up (4 of 4)

Not Implemented

#	Review	Agreed Action	Original due date	Revised due date	Risk rating	Status
5	Contract Management	<p><u>Authorisation of payments</u></p> <p>Guidance for contract management will be updated to include the requirement that Contract Managers authorise payments to supplier before the payment is released. This message will be reiterated in training for Contract Managers. The Accounts Payable team will be reminded that POs can not be produced without authorisation from the relevant staff member.</p>	30/11/2017	31/07/2018	<p>●</p> <p>Medium</p>	Agreed action has not yet been implemented. Due date has been revised to 31/07/2018.
6	Contract Management	<p><u>Contract management framework</u></p> <p>Procurement are working on a framework for contract management across the University. Contracts will be categorised based on impact and the process for managing supplier performance will be tailored to each category. This process will include guidance on the frequency of meetings with suppliers and specify what records should be maintained from these meetings.</p>	31/12/2017	31/07/2018	<p>●</p> <p>Medium</p>	Agreed action has not yet been implemented. Due date has been revised to 31/07/2018.
7	Contract Management	<p><u>Training for contract managers</u></p> <p>Procurement are in the process of developing training for Contract Managers, this will be tailored to individuals based on the impact of the contracts they manage. This will also include introducing touchpoint meetings for high impact contracts. Guidance for contract management will include the process to be followed for terminating contracts.</p>	31/12/2017	31/07/2018	<p>●</p> <p>Medium</p>	Agreed action has not yet been implemented. Due date has been revised to 31/07/2018.

Appendix B: Recent publications and thought leadership

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 alongside our in-house blog which discusses current issues in the education sector. We have included an extract from one of our recent publications.

Students' voice: What would you want from the University of Tomorrow?

In the summer of 2017, we took the opportunity to ask our student interns the question "Reflecting on your experience of higher education and university, what would you want from the university of tomorrow?" and challenged them to work together to bring their ideas to life. Using our 'One' crowdsourcing platform, 370 interns took part and generated 125 ideas and more than 1,000 comments and suggestions.

Key themes:

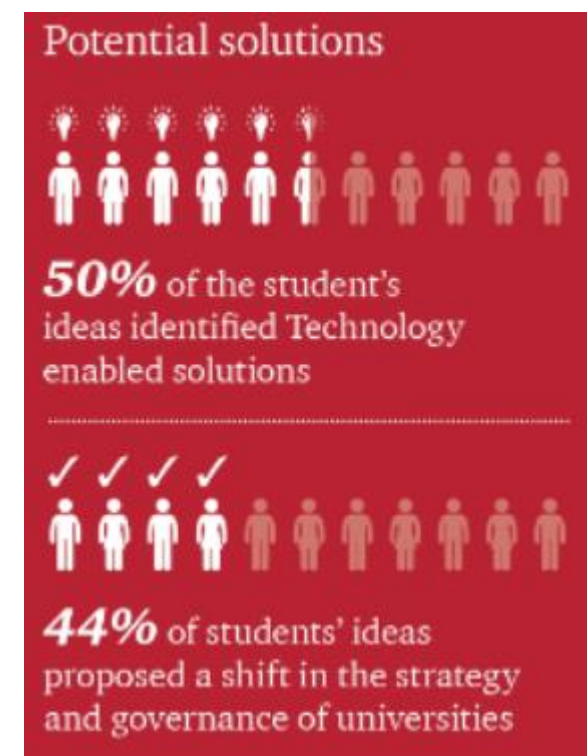
- Using **technology** to solve problems;
- Demanding **transparency** for how University's spend their money;
- The importance of a University's positive **contribution** to the local community;
- The value of **collaboration** and working with individuals from different backgrounds and disciplines;
- The focus on supporting students' **wellbeing** beyond academics, from mental health to housing.

The winning ideas:

1. Inspired by the US-Liberal Arts system, a proposal that students could apply for a specific degree at a university but could also select the Liberal Arts pathway, taking modules from other courses during their first year.
2. An app that helps students find suitable rental accommodation in a way that benefits the students, landlords and their university.

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/ and www.pwc.blogs.com/publicsectormatters/education/



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 16/10/2017. 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 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.

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.

© 2018 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:	Internal Audit Report on Management of Fire Safety.
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Mandy Eddolls – Executive Director of HR
Purpose:	For Information; to provide Committee with the report on the risk, and the related action plan
Which aspect of the Corporate Strategy will this help to deliver?	Safe campus operations affect the entire organisation, but the report findings relate particularly to goal 7 – People & Organisation.
Recommendation:	The Committee is requested to note the report and its findings.

Executive Summary

The report is classified overall as medium risk, with 2 medium risk findings, and 1 low risk finding.

These relate to anecdotal evidence regarding promptness of response to alarms in some areas, lack of a mechanism for tracking the implementation of actions arising from Fire Risk Assessments, and details regarding locations of flammable hazards within buildings, and full details are provided on pages 5-7.

Areas of good practice were identified with respect to action taken following the Grenfell Tower incident, and with regards to linkage with the Southwark emergency planning forum.

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

This page is intentionally left blank

Internal Audit Report 2017/18

Fire Safety Management Review

**London South Bank
University**

Final

January 2018

▶ Click to launch


Page 37

Contents

Executive summary

1 

Background and scope

2 

Findings

Page 38 **3** 

Appendices

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

Distribution list

For action: Mandy Eddolls (Executive Director of Organisational Development and HR)
Ed Spacey (Head of Health, Safety and Resilience)

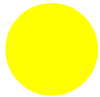
For information: Richard Flatman (Chief Financial Officer)
John Baker (Corporate and Business Planning Manager)



Executive summary

Report classification

Medium 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	-	-	-	-	-
Operating effectiveness	-	-	2	1	-
Total	-	-	2	1	-

Headlines/summary of findings

London South Bank University (LSBU) is planning to release a new fire safety policy. The objective of this audit was to review the processes and controls in place to manage compliance with legislative and regulatory requirements associated with the management of fire related safety risks. The review also explored behaviours and cultures around fire safety.

We identified *two medium and one low risk* operating effectiveness findings relating to fire safety management:

- It is understood from discussions with the security and safety managers that some occupants of buildings are not responding promptly to fire alarms. This is due to a lack of awareness of how quickly fires can spread, in certain pockets around the organisation;
- There is currently no mechanism (such as an action tracker) in place for checking that deficiencies identified as a result of fire risk assessments are being resolved; and
- Emergency plans do not currently contain information regarding what chemical and/or flammable hazards exist within LSBU buildings and where these are located. We understand that a chemical hazards list has been made available to the emergency services but the security and estates teams were not aware of this.

Good practice noted

- Following the Grenfell tower incident, LSBU employed an external company to undertake an independent review of a number of its buildings to evaluate if there was any significant impact following the Grenfell Tower (fatal fire), London, June 2017.
- The Health Safety and Resilience (HSR) team have a proactive and positive relationship with the emergency services, including sitting on the Southwark emergency planning forum.



Background and audit objectives



This review was being undertaken as part of the 2017/18 internal audit plan approved by the Audit Committee.

Background

As the responsible person, under the Regulatory Reform (Fire Safety) Order 2005 (RRFSO) you have a duty to take general fire precautions to ensure, as far as is reasonably practicable, the safety of the people on your premises and in the immediate vicinity. As a result of this legislative requirements all property types need to be considered. There are a number of other legislative requirements that also have a bearing on fire safety be it through construction, health and safety or furnishing activities that providers also need to comply with.

Objective

The objective of this audit was to review the processes and controls in place to manage compliance with legislative and regulatory requirements that pertain to fire. The audit also explored the behaviours and cultures around fire safety. This review was not a technical audit to report on actual levels of compliance with applicable laws and regulations nor on the quality of Fire Risk Assessments performed.

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
12			x	x	X

X = area of primary focus

x = possible area of secondary focus



Fire/Emergency Evacuation

Operating effectiveness

1

Page 4

Finding rating

Rating

Medium

Findings

It is understood from discussions with the Security Team leader and the Health and Safety Manager that in certain areas, some occupants of buildings are not responding promptly to fire alarms when activated. This appears to be due to a gap in training and a lack of awareness of how quickly fires can spread. It is worth noting that this is not the case across all buildings. Certain buildings, the Technopark for example, have very prompt evacuation cultures.

For the new fire policy to be effective, it is incumbent upon every member of staff (as evacuation assistants and where applicable, nominated building controllers) to perform their roles adequately. It is also essential that contractors, visitors and students cooperate effectively with evacuation arrangements.

Implications

Individuals not evacuating buildings when fire alarms sound, are unduly exposing themselves and potentially the emergency services to risk, in the event of a serious fire.

Action plan

- In the short term (Target date 30/01/2018), communication will be sent to staff and students highlighting the importance of responding appropriately to fire alarms and evacuation arrangements.
- As part of the new fire policy implementation, training will be provided to those with fire safety responsibilities.
- The university will continue to take steps to raise awareness of the dangers of not responding to fire alarms/evacuating appropriately. Awareness campaigns will be periodically carried out to ensure all staff, students and visitors are aware of their responsibilities in the event of a fire.
- Where investigation reveals that an alarm has been misused, punitive measures will be considered.

Responsible person/title:

Ed Spacey (Head of Health, Safety and Resilience)

Target date:

30/08/2018

Reference number:

FSM-1

Fire risk assessment (FRA) action plan

Operating effectiveness

2

Page 42

Finding rating

Rating

Medium

Findings

There is currently no mechanism for checking that deficiencies identified as a result of fire risk assessments (FRA) are being tracked, monitored and completed.

We understand that the Estates and Academic Environment (EAE) team are using their long term improvement budget for fixing issues on the FRA Action Plan. This is unsustainable and may require budget injection in the future.

Implications

Without a regular mechanism for checking that actions from fire risk assessments are being completed, there is a risk that actions that are deemed low risk or less important are not being completed, or are not being completed in a timely fashion. In addition, where actions require a resource injection (financial or otherwise), the absence of a review process means that this may not be getting the attention it requires.

Actions not being completed in a timely manner could result in non-compliance with the Regulatory Reform Fire Safety order 2005. In addition, if actions are not being completed as a result of resource constraints, this needs to be flagged and brought to the attention of responsible parties. Ultimately, incomplete actions undermine the effectiveness of the FRA process.

Action plan

- The EAE team will provide a Fire Action Plan status update to the EAE Senior Management team periodically (at least every quarter). This should reflect what is entered into the concept system and the progress made against each agreed action.
- HSR team will include a KPI for FRA actions completed/outstanding in the annual H&S reports provided to the executive board.

Responsible person/title:

David Murray (Head of Estates) /Ed Spacey (Head of Health, Safety and Resilience)

Target date:

30/06/2018

Reference number:

FSM-2

Communication of chemicals hazards list to first responders

Operating effectiveness

3

Page 43

Finding rating

Rating

Low

Findings

The emergency plans do not currently contain information regarding what chemical and/or flammable hazards exist within LSBU buildings and where these are located. Examples of this could be an LPG gas cylinder or dangerous chemicals in a laboratory. We understand that there is a chemical hazards list which has been provided to the emergency services. However, the estates and security teams (stakeholders in the fire first response process) did not seem to be aware of the existence of this information.

Implications

In the event of a fire, a first responder could access a part of the building where a flammable substance or other chemical hazard exists. This could lead to them inadvertently putting themselves at risk unduly.

Action plan

- The chemical hazards list will be shared with first responders (security officers).
- Schools and areas dealing with chemicals must keep an accurate and up-to-date chemicals hazards list and need to ensure that they've supplied this list to the HSR team. This is particularly applicable to the engineering and applied sciences faculties.

Responsible person/title:

Ed Spacey (Head of Health, Safety and Resilience)

Dean of School Engineering (liaising with any other Deans necessary)

Dean of Applied Sciences

Target date:

30/01/2018

Reference number:

FSM-3

**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

Appendices

Page 44

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 A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

Appendix B: Terms of reference

Fire Safety Management

To: Mandy Eddolls - Interim Executive Director of Organisational Development and HR
From: Justin Martin – Head of Internal Audit

Page 47

Background and audit objectives



This review is being undertaken as part of the 2017/18 internal audit plan approved by the Audit Committee.

Background

As the “responsible person”, under the Regulatory Reform (Fire Safety) Order 2005 (RRFSO) you have a duty to take general fire precautions to ensure, as far as is reasonably practicable, the safety of the people on your premises and in the immediate vicinity. Between the two legislative requirements all property types need to be considered. There are a number of other legislative requirements that also have a bearing on fire safety be it through construction, health and safety or furnishing activities that providers also need to comply with.

Objective

The objective of this audit is to review the processes and controls in place to manage compliance with legislative and regulatory requirements around fire. The audit will also look to explore behaviours and cultures around fire safety. This review is not a technical audit to report on actual levels of compliance with applicable laws and regulations nor on the quality of Fire Risk Assessments (FRA) performed.

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
12			x	x	X

X = area of primary focus

x = possible area of secondary focus

Audit scope and approach (1 of 3)



Scope

We will review the design and operating effectiveness of key controls in place relating to Fire Safety. The sub-processes and related control objectives included in this review are:

Sub-process	Objectives
Governance Framework	<ul style="list-style-type: none"> Formal assignment of roles and responsibilities has taken place and reporting lines are clearly defined. Approved policies and procedures governing the organisation’s strategy, approach to and controls over Fire Safety Management are in place.
Data quality	<ul style="list-style-type: none"> Management can evidence that a complete and accurate record of all properties containing communal areas, including voids, is maintained. Additions/deletions to the property portfolio are appropriately reflected, in a timely manner, in the FRA population.
Training and qualifications	<ul style="list-style-type: none"> All staff who have responsibility for fire safety management and any control measures have received training that the organisation has deemed appropriate to equip staff and/or contractors with the required levels of competence. Where external contractors are used to undertake any aspects of fire safety management, the organisation has sought assurances that the contractors are appropriately skilled/qualified.
Fire Risk Assessment process	<ul style="list-style-type: none"> A programme is in place to identify FRAs falling due (on new or existing properties), to schedule assessments to fall within the timescales set out by the relevant policy. Circumstances that would require an update to a FRA have been defined (for example change in use or design of a building) and there are appropriate processes in place to identify those and schedule FRAs to be undertaken. All FRAs undertaken are recorded centrally in a timely manner. Deficiencies noted in FRAs are recorded centrally, actioned and tracked through to completion, within appropriate timescales.

Audit scope and approach (2 of 3)



Sub-process	Objectives
Regular testing and servicing	<ul style="list-style-type: none"> • Policies and procedures for periodic fire safety equipment and procedure testing (for example fire alarm testing, inspection and servicing of safety equipment, fire drills and review of guidance provided in the event of fire) are in place and are adhered to.
Incident reporting	<ul style="list-style-type: none"> • Training and awareness campaigns are periodically carried out to ensure all staff and residents are aware of their responsibilities for fire safety as well as knowing how to recognise and report incidents. • A central log of incidents is maintained and available to all those responsible for fire safety. • There are formal lessons learned / continuous improvement activities in place to re-assess risks as a result of previous incidents.
Monitoring and reporting	<ul style="list-style-type: none"> • Senior Management and the Board receive regular, timely and complete information regarding the performance of the Fire Management process against legislative requirements as well as details of any incidents or enforcement notices. • Appropriate escalation procedures are in place to ensure that management and the Board are made aware of any incidents/performance issues that are deemed to impact the organisations ability to manage fire safety.
Quality Assurance	<ul style="list-style-type: none"> • A formal quality assurance process is in place whereby independent assurance is provided over the completeness and quality of Fire Risk Assessments and the associated remedial actions.

Audit scope and approach (3 of 3)



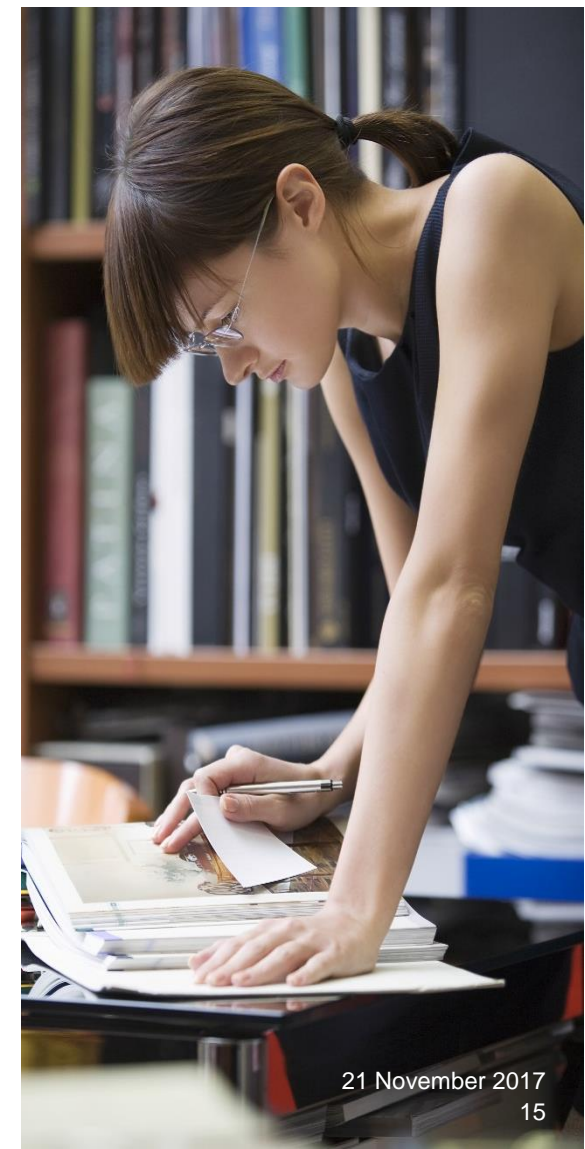
Limitations of scope

This review is limited to the design and operating effectiveness of controls over the areas outlined above. It is not a technical review of the quality of works performed in accordance with relevant laws and regulations.

Audit approach

Our audit approach is as follows:

- Obtain an understanding of the Fire Risk Management arrangements through discussions with key personnel and review of systems documentation.
- Identify the key risks with the Fire Risk Management process
- Evaluate the design of the controls in place to address the key risks.



Internal audit team and key contacts



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	Telephone: 0207 212 4269 Email: justin.f.martin@pwc.com
Lucy Gresswell	Engagement Manager	Telephone: 07718 098 321 Email: lucy.j.gresswell@pwc.com
Phil Davis	Health & Safety Specialist	Telephone: 07595 850 798 Email: phil.davis@uk.pwc.com
Dola Faseun	Health & Safety Auditor	Telephone: 07841803124 Email: dola.faseun@pwc.com

Key contacts – London South Bank University

Name	Title	Contact details	Responsibilities
Mandy Eddolls	Executive Director of Organisational Development and HR (Audit Sponsor)	0207 815 6224 eddollsm@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

Timetable



Timetable

Fieldwork start	21 September 2017
Fieldwork completed	6 October 2017
Draft report to client	13 October 2017
Response from client	20 October 2017
Final report to client	26 October 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 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 16 October 2017. 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 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.

© 2018 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:	Internal Audit Continuous Audit Report into Student Data
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	For Information; to provide Committee with the latest report into the continuous audit of the controls around Student Data.
Which aspect of the Corporate Strategy will this help to deliver?	Effective enrolment and records management for student activity involves the entire organisation, but the report findings relate particularly to goal 1, Teaching & Learning, % - International, and 8 – Resources & Infrastructure.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Executive Summary

The report is classified overall as medium risk, with 41 identified exceptions, comparable with the previous report, and with 2 control design recommendations.

A majority of these findings are against control S2, where some exceptions are historical, and relate to a period before the revised policy and process was implemented, or relate to local good practice process that exceeds regulatory requirements.

The control design relates to the use of the new Haplo software system for PHD management, which will enable the recording of attendance records for international students

The detailed findings are covered on pages 5 – 12, with management responses.

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

This page is intentionally left blank

Internal Audit Report 2017/18

Continuous Auditing: Student Data 2017/18 – Period 1

London South Bank
University

Final

January 2018

▶ Click to launch


Page 59

Contents

Executive summary

1 

Background and scope

2 

Findings

Page **3** 

Appendices

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

Distribution list

For action: Ralph Sanders (Director of Planning, Information & Reporting)
Lisa Upton (Head of Registry)
Neil Gillett (Immigration and International Student Advice Manager)
Alan Butt (Student Engagement Team Leader)

For information: Richard Flatman (Chief Financial Officer)
John Baker (Corporate and Business Planning Manager)
Jamie Jones (Head of Student Administration)
Andrew Ratajczak (Manager: Fees, Bursaries and Central Enrolment)
Natalie Ferer (Financial Controller)
Audit Committee



Executive summary



System Classification

Medium Risk



System Summaries

The table below summarises the overall performance rating for student data this period. This is based on the number and severity of findings identified each period. Our rating criteria is set out in Appendix A. This shows that performance in the current period is consistent with previous period: 41 operating effectiveness exceptions were identified in both Period 1 2017/18 and Period 2 2016/17. The testing results suggest that there has been a decline in performance for S2 (Tier 4 controls). The performance for the majority of other control areas has improved. One control design exception were also identified in Period 1 2017/18 (Period 2 2016/17: 1 exception).

Control	P1 17/18 Effectiveness	P1 17/18 Control design	P2 16/17 Effectiveness	P2 16/17 Control design	Trend
S1	11	-	14	-	↑
S2	16	1	-	-	↓
S3	4	-	1	-	↓
S4	-	-	1	-	↑
S5	2	-	6	-	↑
S6	3	-	5	-	↑
S7	1	-	-	1	↓
S8	4	-	8	-	↑
S9	-	-	1	-	↑
S10	-	-	5	-	↑
Total	41	1	41	1	↔

Background and scope



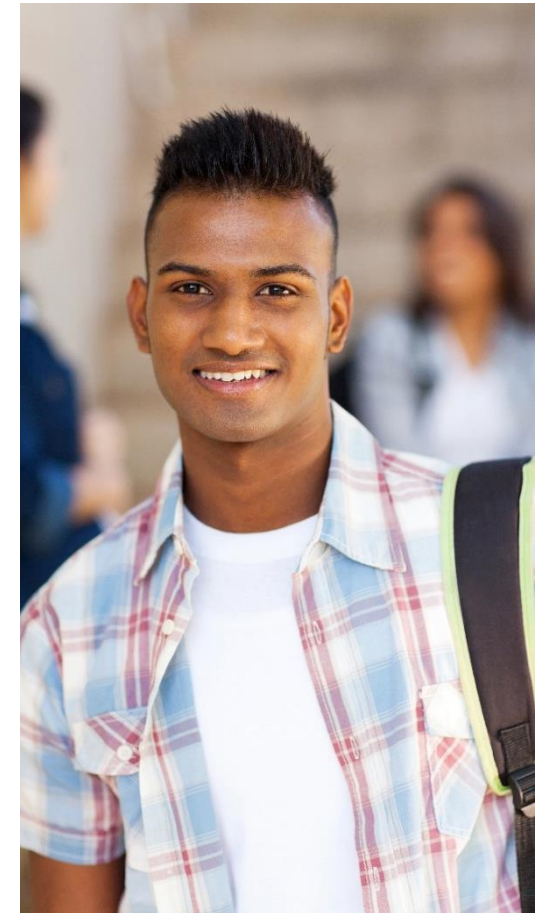
Background

The Higher Education Funding Council for England’s (HEFCE) Memorandum of Assurance and Accountability (MAA) states that the Audit Committee is required to produce an annual report for the governing body and the accountable officer. This report must include the committee’s opinion on the adequacy and effectiveness of the University’s arrangements for management and quality assurance of data submitted to the Higher Education Statistics Agency (HESA), the Student Loans Company (SLC), HEFCE and other bodies. Whilst there is no requirement for our internal audit programme to provide a conclusion over data quality, our internal audit programme for 2017/18 has been designed to support the Audit Committee in forming its conclusion.

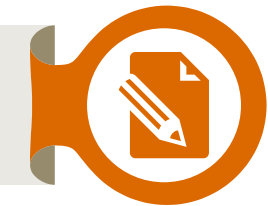
Our Student Data Continuous Audit programme tests key controls associated with data quality on an on-going basis to assess whether they are operating effectively and to flag areas and/or report transactions that appear to circumvent controls.

We have outlined the specific controls we have tested in the Terms of Reference (please refer to Appendix B). These have been identified through our annual audit planning process and meetings with management. We will continue to refresh this knowledge throughout the year to ensure we focus upon the key risks facing London South Bank University (LSBU).

A summary of our findings and the matters arising in the course of our work this period is set out in the Executive Summary. Our detailed findings are set out in the Findings section.



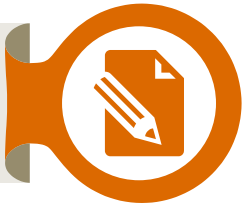
Detailed Findings (1 of 7)



	Key Control	Exceptions P1 2017/18*	Details on exceptions	Management Comment
S1	<p>New Student Record</p> <p>Following a student record being created in QLS at the application stage, appropriate checks are performed prior to fully enrolled ('EFE') status. These checks include:</p> <ul style="list-style-type: none"> • A full ID check • Criminal conviction check (self-declaration by students) • Entry criteria have been met 	<p>11</p>	<ul style="list-style-type: none"> • For 10/25 new students tested, there was no evidence that a criminal conviction check has been completed. • For 1/25 new students, the LSBU faculty member did not date the enrolment form, therefore we cannot confirm that all checks were made prior to EFE status. 	<p>Management response and action:</p> <p>A review of application systems is being undertaken and work is being carried out to address issues identified that resulted in these errors.</p> <p>Owner:</p> <p>Lisa Upton, Head of Registry</p> <p>Due date:</p> <p>31/05/2018</p>

**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 (1 of 7)



Page 64

	Key Control	Exceptions P1 2017/18*	Details on exceptions	Management Comment
S2	<p>Tier 4 controls</p> <p>Supporting documentation is obtained and retained to ensure Tier 4 requirements are met.</p>	<p>16</p>	<ul style="list-style-type: none"> For 7/25 students, the passport held for the student had expired (a). For 1/25 students, not all relevant pages of the passport were held (b). For 2/25 students, we identified that the student had changed course, but this had not been communicated to the Home Office (c). <p><i>Continued on page 7.</i></p>	<p>Management response and action:</p> <p>Holding a valid passport on file is not a Home Office requirement. However, we recommend students do get updated passports to ensure they can travel (a).</p> <p>This is historical. New processes have been put in place to ensure we take all copies and keep them on file at enrolment(b).</p> <p>This is historical. We did not have a process in place at the time to identify these. New processes have been put in place to ensure these are not missed (c).</p>

**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 (2 of 7)



	Key Control	Exceptions P1 2017/18	Details on exceptions	Management Comment
S2	<p>Tier 4 controls</p> <p>Supporting documentation is obtained and retained to ensure Tier 4 requirements are met.</p>	<p>16</p>	<ul style="list-style-type: none"> For 3/25 students, there was no record of the student's attendance. This is because the student has progressed to the dissertation stage of their course and attendance records are not maintained for this stage (d). For 1/25 students there was no evidence that the student had completed a TB test (e). For 1/25 students there was no evidence of a completed Immigration Information Form (f). For 1/25 students, the university did not hold current contact details for the student (g). 	<p>Management response and action:</p> <p>This has been referred back to the Student Administration team for investigation and action (d).</p> <p>Holding a record of the TB test is not a Home Office requirement. We ensure we check this and keep it on file to reduce the risk of refusal (e).</p> <p>Keeping the Immigration Form on file is not a Home Office requirement. We ensure we check this and keep it on file to reduce the risk of refusal (f).</p> <p>We collect this information at enrolment but it is dependent on students having UK telephone number at the time and sometimes they haven't arranged this. We send monthly emails to chase up this information but it relies wholly on the student providing this information (g).</p> <p>Owner and due date:</p> <p>Neil Gillet, Immigration and International Student Advice Manager, 31/05/2018.</p>

Detailed Findings (3 of 7)



	Key Control	Exceptions P1 207/18	Details on exceptions	Management Comment
S3	<p>Student Engagement</p> <p>Applies to all Schools (other than Health & Social Care and students with Tier 4 visas).</p> <p>Engagement data is captured in the Student Point of Contact (SPOC) report. The following indications of engagement are monitored:</p> <ul style="list-style-type: none"> •Entry onto campus. •Moodle use. •Attendance at teaching sessions. •Submission of assessment •MyLSBU use. <p>Students failing to meet the minimum thresholds for engagement are investigated.</p>	4	<p>4/25 exceptions noted.</p> <p>All 4 exceptions relate to the first step in the escalation process "email 1" not being sent within one week of the student failing to meet the minimum engagement criteria.</p>	<p>Management response and action:</p> <p>Student Engagement team to ensure engagement written procedure is followed. All exceptions noted relate to one school where there was a new member of staff in place. This new member of staff is now up-to-date on the process.</p> <p>Owner:</p> <p>Alan Butt, Student Engagement Team Leader</p> <p>Due date:</p> <p>31/05/2018</p>

Detailed Findings (4 of 7)



Key Control	Exceptions P1 2017/18	Details on exceptions	Management Comment
<p>S4 Student Attendance</p> <p>Applies to School of Health & Social Care and students with Tier 4 visas.</p> <p>Attendance reports from the Student Attendance Monitoring system (SAM) are generated by the School of Health & Social Care and for students with Tier 4 visas to identify periods of non-attendance. Students failing to meet the minimum attendance thresholds are investigated.</p>	<p>0</p>	<p>No exceptions noted.</p>	
<p>S5 Course Changes</p> <p>Supporting evidence is obtained prior to processing any course changes or withdrawals.</p>	<p>2</p>	<ul style="list-style-type: none"> For 1/25 students there was no evidence that the change in course form had been completed. For 1/25 students, the course director did not date the form when the change in course form was signed. We are therefore unable to confirm whether or not the change was actioned after all required approvals had been provided. 	<p>Management response and action:</p> <p>A training session for student admin on the course change process was delivered in June 17. Spot checks are made on course change requests and failures raised with staff and their line managers.</p> <p>Owner and due date:</p> <p>Lisa Upton, Head of Registry, 31/05/2018.</p>

Detailed Findings (5 of 7)



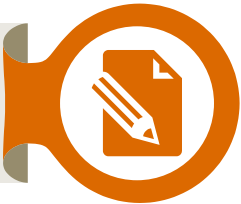
	Key Control	Exceptions P1 2017/18	Details on exceptions	Management Comment
S6	<p>Withdrawals</p> <p>Supporting documentation is retained for all change of circumstances. Changes of circumstances are processed on a timely basis.</p> <p>This testing is restricted to the testing of withdrawals.</p>	3	<ul style="list-style-type: none"> For 2/20 withdrawals, there was no evidence that the student requested to be withdrawn. We have seen withdrawal forms completed by the course director in respect of these withdrawals but no evidence from the student themselves. For 1/20 withdrawals, the withdrawal was not processed within a timely manner. The target is for withdrawals to be processed in 14 days, it took 19 days for the withdrawal to be completed. 	<p>Management response and action:</p> <p>These two withdrawals were actioned by the course director for the HSC apprentice course. The students had left the employment of the Trust and therefore withdrawal forms were difficult to get completed. A review of the process to be followed in this circumstance is being considered along with all Apprentice processes.</p> <p>Owner and due date:</p> <p>Lisa Upton, Head of Registry, 31/05/2018.</p>
S7	<p>Module Data Exception Reporting</p> <p>Exception reports are run to identify changes made to student module data and are investigated.</p>	1	<p>No exception reports were produced in the testing period. As such an exception has been noted.</p> <p>We have seen that the November 2017 exception report was run and management intends to generate these reports every two months going forwards.</p>	<p>Management response and action:</p> <p>Exception reports were being run on an adhoc basis. A change to this process has now been made to produce reports every two months to review and improve the quality and accuracy of record keeping.</p> <p>Owner and due date:</p> <p>Lisa Upton, Head of Registry, 31/05/2018.</p>

Detailed Findings (6 of 7)



	Key Control	Exceptions P1 2017/18	Details on exceptions	Management Comment
S8	<p>Changes to Module Data</p> <p>Evidence is retained to support any changes to student module data.</p>	<p>4</p>	<p>We reviewed the November 2017 exception report. We found 4/20 students were registered to a different number of credits than expected.</p> <ul style="list-style-type: none"> For 2/20 students, no explanation was provided for the difference. For 1/20 students, it was identified that the course is showing the incorrect number of credits. This had not been resolved at the time of audit fieldwork. For 1/20 students, it was confirmed that the student had been registered to the incorrect number of credits, but this had not been resolved at the time of audit fieldwork. 	<p>Management response and action:</p> <p>The audit was undertaken midway through the responses from student admin being reviewed and issues identified and outstanding actions being followed up on.</p> <p>Owner and due date:</p> <p>Lisa Upton, Head of Registry, 31/05/2018.</p>
S9	<p>QLS: New Starters</p> <p>All new users of the QLS system must complete an authorisation form which is authorised by their line manager and IT prior to system access.</p>	<p>0</p>	<p>No exceptions noted.</p>	

Detailed Findings (7 of 7)



	Key Control	Exceptions P1 2017/18	Details on exceptions	Management Comment
S10	<p>QLS: Leavers</p> <p>Leavers are removed from the QLS system on a timely basis.</p>	0	No exceptions noted.	

Attendance records for Tier 4 PhD students (S2)
Control design

1

Findings

Tier 4 requirements state that attendance records must be retained for all Tier 4 students. We identified that attendance records are not maintained for PhD students.

Implications

Without attendance records for PhD students the university runs the risk of non-compliance with UKVI requirements.

Action plan

Haplo Monitoring Records for PhD students are maintained, however at the time of the audit fieldwork, staff with access to this system weren't available. Additional access rights will be set up to ensure that staff can confirm compliance with the Tier 4 regulations.

Responsible person/title:

Louise Thompson, Research Degrees Programme Manager

Target date:

28/02/2018

Reference number:

1

Page 7

Finding rating

Rating

Medium risk



**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

Appendices

Page 72

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

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: Student Data 2017/18

To: Richard Flatman – Chief Financial Officer

From: Justin Martin – Head of Internal Audit

Page 75

Background and audit objectives (1 of 2)



This review is being undertaken as part of the 2017/2018 internal audit plan approved by the Audit Committee.

Background and audit objectives

The Higher Education Funding Council for England’s (HEFCE) Memorandum of Assurance and Accountability (MAA) states that the Audit Committee is required to produce an annual report for the governing body and the accountable officer. This report must include the committee’s opinion on the adequacy and effectiveness of the University’s arrangements for management and quality assurance of data submitted to the Higher Education Statistics Agency (HESA), the Student Loans Company, HEFCE and other bodies. Whilst there is no requirement for our internal audit programme to provide a conclusion over data quality, our internal audit programme for 2017/18 has been designed to support the Audit Committee in forming its conclusion.

Our Student Data Continuous Audit programme will test key controls associated with data quality 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 will be undertaken twice a year and provide 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.

Background and audit objectives (2 of 2)



Background and audit objectives

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 2)

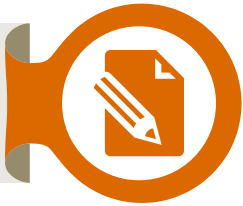


Scope

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
Student Systems	Complete and accurate records of students and their activity are maintained.	<ul style="list-style-type: none"> Application and enrolment data may be inaccurate. This could also result in fees not being correct resulting in students being over or undercharged and an associated impact on income. UKVI requirements are not complied with. This could result in London South Bank University losing their license to operate affecting fee income and leading to reputational damage. Student engagement or attendance records are incorrect undermining the reliability of management information. Course changes are not identified on a timely basis which could affect fee income, as well as student data quality. Reporting of changes in circumstances to the SLC are not reported and processed accurately, completely and on a timely basis. This could mean student data is inaccurate. Student module data is inaccurate or incomplete, undermining the reliability of data. Users have unauthorised access and can make inappropriate amendments to student records which could compromise the validity, accuracy and completeness of student data.

Audit scope and approach (2 of 2)



Limitations of scope

Our work is not intended to provide assurance over the effectiveness of all the controls operated by management over student data; 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 2017/18:

- Phase 1: April 2017 – October 2017
- Phase 2: November 2017 – March 2018



Internal audit team



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@pwc.com
Lucy Gresswell	Engagement Manager	07718 098 321 lucy.j.gresswell@pwc.com
Janak Savjani	Continuous Auditing Supervisor	07802 660 974 janak.j.savjani@pwc.com
Josh Thomas	Continuous Auditing Technician	07718 978628 joshua.thomas@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
Andrew Ratajczak	Manager; Fees, Bursaries and Central Enrolment	ratajca@lsbu.ac.uk	Hold initial scoping meeting Review and meet to discuss issues arising and develop management responses and action plan
Neil Gillett	Immigration and International Student Advice Manager	neil.gillett@lsbu.ac.uk	
Nuria Prades	Senior International Officer (UK & non-EU Europe)	pradesn@lsbu.ac.uk	
Lisa Upton	Deputy Academic Registrar (Acting)	uptonl@lsbu.ac.uk	
Dave Lewis	Software Development Team Leader	dave.lewis@lsbu.ac.uk	Audit Contact

Key contacts

Key contacts – London South Bank University

Name	Title	Contact details	Responsibilities
Jamie Jones	Head of Student Administration	jamie.jones@lsbu.ac.uk	Audit contact
Alan Butt	Student Engagement Team Leader	butttab@lsbu.ac.uk	Audit contact
Sheila Patel	Applications Support and Maintenance Team Leader	sheila@lsbu.ac.UK	Audit contact
Natalie Ferer	Financial Controller	ferern@lsbu.ac.uk	Audit contact



Timetable



Timetable

	Phase 1	Phase 2
Fieldwork start	04/12/2017	09/04/2018
Fieldwork completed	15/12/2017	20/04/2018
Draft report to client	05/01/2018	04/05/2018
Response from client	19/01/2018	18/05/2018
Final report to client	26/01/2018	25/05/2018

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 key student data controls at London South Bank University 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. The deliverables required to complete testing of the controls is outlined in appendix 2.

Our testing will be applicable to all students, with the exception of Tier 4 controls which is only relevant to international students.

Enrolment

Key risk	Key Control	Reference
Application and enrolment data may be inaccurate. This could also result in fees not being correct resulting in students being over or undercharged and an associated impact on income.	Following a student record being created in QLS at the application stage, appropriate checks are performed prior to fully enrolled ('EFE') status. These checks include: <ul style="list-style-type: none"> • A full ID check • Criminal conviction check (self-declaration by students) • Entry criteria have been met Key contact: Lisa Upton	S1
UKVI requirements are not complied with. This could result in London South Bank University losing their license to operate affecting fee income and leading to reputational damage.	Supporting documentation is obtained and retained to ensure Tier 4 requirements are met. Key contact: Neil Gillett and Nuria Prades	S2

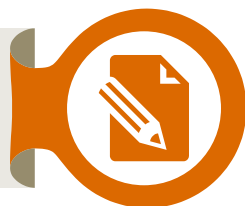
Appendix 1: Key controls schedule



Student Attendance Monitoring

Key risk	Key Control	Reference
Student engagement or attendance records are incorrect undermining the reliability of management information.	<p><u>Student Engagement</u></p> <p><i>Applies to all Schools (other than Health & Social Care and students with Tier 4 visas).</i></p> <p>Engagement data is captured in the Student Point of Contact (SPOC) report. The following indications of engagement are monitored:</p> <ul style="list-style-type: none"> • Entry onto campus. • Moodle use. • Attendance at teaching sessions. • Submission of assessment • MyLSBU use. <p>Students failing to meet the minimum thresholds for engagement are investigated.</p> <p>Key contact: Alan Butt, Student Engagement Team Leader</p>	S3
	<p><u>Student Attendance</u></p> <p><i>Applies to School of Health & Social Care and students with Tier 4 visas</i></p> <p>Attendance reports from the Student Attendance Monitoring system (SAM) are generated by the School of Health & Social Care to identify periods of non-attendance. Students failing to meet the minimum attendance thresholds are investigated.</p> <p>Key contact: Alan Butt, Student Engagement Team Leader</p>	S4

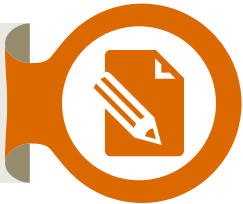
Appendix 1: Key controls schedule



Enrolment Amendments

Key risk	Key Control	Reference
Course changes are not identified on a timely basis this could affect fee income.	Supporting evidence is obtained prior to processing any course changes or withdrawals. Key contact: Andrew Ratajczak	S5
Reporting of changes in circumstances to the SLC are not reported and processed accurately, completely and on a timely basis. This could mean student data is inaccurate.	Supporting documentation is retained for all change of circumstances. Changes of circumstances are processed on a timely basis. This testing is restricted to the testing of withdrawals. Key contact: Andrew Ratajczak	S6
Student module data is inaccurate or incomplete, undermining the reliability of data.	Exception reports are run to identify changes made to student module data and are investigated. Key contact: Lisa Upton	S7
	Evidence is retained to support any changes to student module data. Key contact: Lisa Upton	S8
	All new users of the QLS system must complete an authorisation form which is authorised by their line manager and IT prior to system access. Key contact: Lisa Upton	S9

Appendix 1: Key controls schedule



System Access

Key risk	Key Control	Reference
Users have unauthorised access and can make inappropriate amendments to student records which could compromise the validity, accuracy and completeness of student data.	Leavers are removed from the QLS system on a timely basis. Key contact: Lisa Upton	S10

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 16 October 2017. 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 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.

© 2018 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:	Internal Audit Continuous Audit Report into Key Financial Systems (period 2 – August – December 2017).
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	PriceWaterhouse Coopers
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	For Information; to provide Committee with the latest report into the continuous audit of the controls around Key Financial Systems.
Which aspect of the Corporate Strategy will this help to deliver?	Effective financial management and operations involve the entire organisation, but the report findings relate particularly to goal 8 – Resources & Infrastructure.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Executive Summary

The report finds overall improvement in the tested areas from the period 1 report, with Payroll and Accounts Payable improving to green, Cash and General Ledger remaining green, and slight decline to amber in Accounts Receivable.

The exception findings are detailed on pages 5 to 29, with related control design findings relating mainly to articulation or amendment of current process, including revised journal process, AR checklists, supplier duplicate checking and revised amendment process, and a KX user access process which has already been introduced. The implementation of these will be tracked through the 4-Action tracking platform alongside other report findings.

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

This page is intentionally left blank

Internal Audit Report 2017/18

Continuous Auditing: Key Financial Systems 2017/18 – Phase 2

*London South Bank
University*

February 2018

Final

▶ Click to launch


Page 93

Contents

Executive summary

1 

Background and scope

2 

Findings

Page 94 **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

Overall, we are pleased to report that there has been an improvement in the performance of key financial systems in the current period. We have seen a marked improvement in the performance of payroll with fewer exceptions identified across all HR and payroll controls compared to the previous period. The performance of Accounts Payable has also improved with fewer exceptions in the current period. We have moved the risk rating of Accounts Receivable to amber as we identified a number of instances where debts were not chased in accordance with the debt recovery policy. The performance of Cash and General Ledger remains green. Our ratings are based on the number and severity of findings noted for controls tested as part of the programme.

The below summary does not include control design issues which are individually risk rated. We identified seven control design findings – one finding was rated high risk, three findings were rated medium risk and three findings were rated low risk.

Our detailed findings are set out in Findings section of this report, starting on page 5. Our rating criteria are set out at Appendix A.

System / Rating	P2 2017/18	P1 2017/18	P2 2016/17	P1 2016/17	P2 2015/16	P1 2015/16	Trend
Payroll	Green	Red	Amber	Amber	Amber	Green	
Accounts Payable	Green	Amber	Amber	Green	Green	Green	
Accounts Receivable	Amber	Green	Green	Green	Green	Green	
Cash	Green	Green	Green	Amber	Green	Green	
General Ledger	Green	Green	Green	Amber	Green	Green	

Background and scope



Background

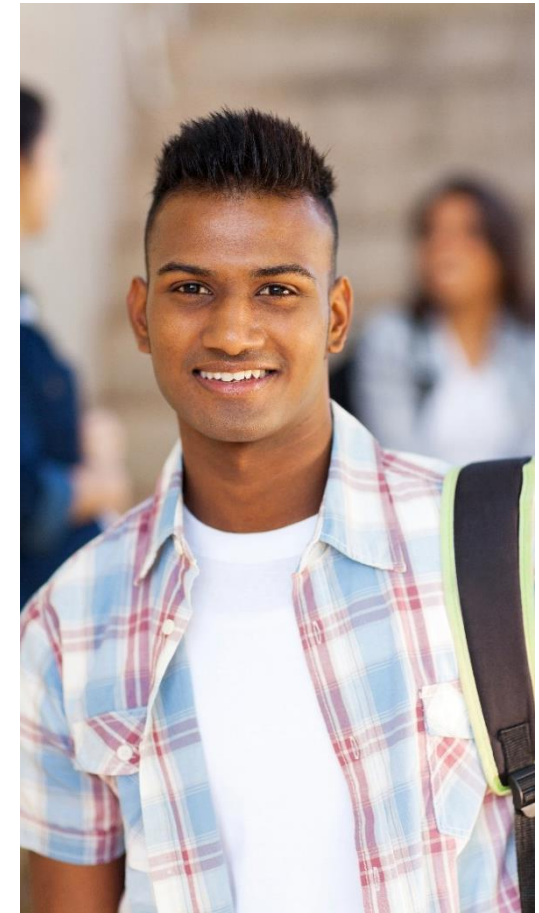
The purpose of our Continuous Auditing programme is to test key controls on an on-going basis to assess whether they are operating effectively and to flag areas and/or report transactions that appear to circumvent controls. The systems included within the scope of our work in 2017/18 are:

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

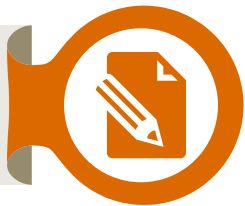
We have outlined the controls we tested in Appendix B. These have been identified through our annual audit planning process and meetings with management to update our understanding of the control framework in place. We will continue to refresh this knowledge throughout the year to ensure we focus upon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

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	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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"> 5/20 new starter forms were authorised after the employee had commenced employment. In one instance the new starter form was approved 21 days after the employee's start date. In all 5 instances, the employee was not paid until after the authorisation had occurred. <p>Management response:</p> <p>The current audit is looking at the approval process for new starters based on the assumption that new starters should be approved prior to start date. During the design and implementation of iTrent, the approval part of the system was designed with the payroll deadline day as the key date for this process.</p> <p>Since implementation, the team has been following this process and new starters are approved prior to the payroll deadline day following start date. In each and every case listed this occurred within time and full authorisation provided, and there was therefore no financial implication.</p> <p>The Recruitment Team are currently documenting these processes within a Recruitment Process Manual for launch in Quarter 2.</p> <p>Responsibility for action:</p> <p>David Lee, HR Systems & Analytics Manager</p>	●	●	●	●

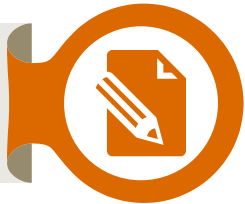
Detailed Findings



Payroll

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
P2 Leaver documentation, including evidence of line manager approval, is received from Human Resources upon notification of resignation or redundancy.	●		●	●	●	●
P3 The BACS run is reviewed by the Financial Controller and a Payment Release Form completed.	●		●	●	●	●

Detailed Findings

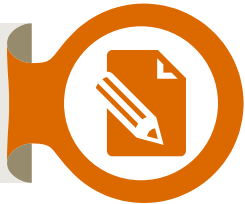


Payroll

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
P4	●	Exception reports are produced and reviewed as part of month-end procedures, before the payment run is authorised.*	●	●	●	●
P5	●	Variation forms, with supporting documentation, are received prior to any changes being made to standing data.	●	●	●	●

* 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.

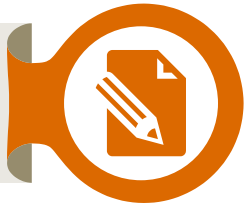
Detailed Findings



Payroll

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
P6 Access to the payroll system is restricted to appropriate personnel.	●		●	●	●	●
P7 Appropriately authorised overtime claim forms and timesheets are received prior to payment being made.	●		●	●	●	●

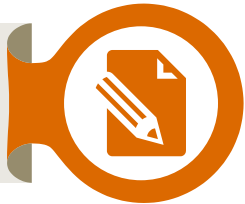
Detailed Findings



Payroll

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●		●	●	●	●
P9 Expenses are supported by appropriately authorised claim forms.	●	<ul style="list-style-type: none"> For 2/25 expense forms, the approver did not date the expense form, we are therefore unable to confirm that approval was granted prior to the payment being made. <p>Management response: Staff continue to be reminded of their responsibility to date expense forms when they are approved.</p> <p>Responsibility for action: Natalie Ferer, Financial Controller</p>	●	●	●	●

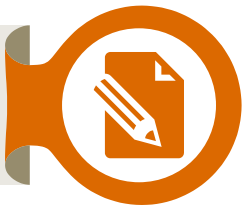
Detailed Findings



Accounts Payable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●	●	●	●

Detailed Findings



Accounts Payable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
AP3 Invoices are matched to purchase orders for all expenditure prior to payment and variances investigated.	●	<ul style="list-style-type: none"> For 1/25 invoices paid, a purchase order had not been raised in respect of the expenditure. <p>Management response:</p> <p>The invoice should have been paid against a PO. This was an old invoice and the PO originally raised did not have funds left to cover this bill. It was agreed that we would process it uncommitted as an exception. The supplier is aware that they should only accept orders made with an official PO.</p> <p>Responsibility for action:</p> <p>Natalie Ferer, Financial Controller</p>	●	●	●	●

Detailed Findings



Accounts Payable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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 3/20 suppliers tested, a duplicate supplier existed on the system with an identical supplier name. A control design weakness has also been raised in respect of the controls for preventing duplicate suppliers. <p>Management response:</p> <p>We will implement the control design findings to increase controls in this area, and increase the frequency of checks made.</p> <p>Responsibility for action:</p> <p>Penny Green (Head of Procurement)</p>	●	●	●	●

Detailed Findings



Accounts Payable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●		●	●	●	●

AP1: Supplier amendments

Control Design

1

Page 106

Finding rating

Rating

High

Findings

There is no audit trail to evidence that appropriate checks have been made to validate the authenticity of requests to amend supplier details.

Implications

Invalid or fraudulent supplier details could be recorded on Agresso. Incorrect supplier details could be used to confirm fraudulent requests to amend bank details.

Agreed action

We will keep a record of contact made with the supplier to confirm that requests to amend supplier details are genuine.

Responsible person/title:

Penny Green (Head of Procurement)

Target date:

28/02/2018

Reference number:

1

AP1: Authorisation of new suppliers and amendments to supplier details

Control Design

2

Page 107

Finding rating

Rating

Medium

Findings

We identified a weakness in the segregation of duties controls for adding new suppliers and amending supplier details in Agresso. When a new supplier is added, or a change is made to the supplier record, the change is reflected instantaneously in Agresso – meaning that validation by a second member of staff is completed after the change has been made in the system.

Implications

Invalid suppliers, or incorrect supplier standing data, is maintained leading to inaccurate or fraudulent payments.

Agreed action

We will introduce additional steps whereby the supplier account is deactivated immediately after being set up on the system. This means that payments can not be made until the change is validated by a second member of staff.

Responsible person/title:

Penny Green (Head of Procurement)

Target date:

28/02/2018

Reference number:

2

AP5: Duplicate suppliers

Control Design

3

Page 108

Finding rating

Rating

Low

Findings

We identified duplicate suppliers in our testing. The system does not allow duplicate suppliers with identical details to be set up, but where there is a slight difference in the supplier record (i.e. “Company X Limited” or “Company X Ltd”), another supplier record can be set up.

Implications

Amounts due to suppliers for goods and services are over paid.

Agreed action

A monthly report will be run on supplier details (i.e. bank details, contact details etc) to identify any duplicate records.

Responsible person/title:

Penny Green (Head of Procurement)

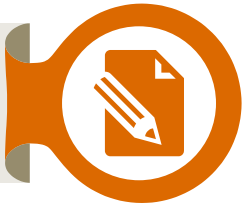
Target date:

28/02/2018

Reference number:

3

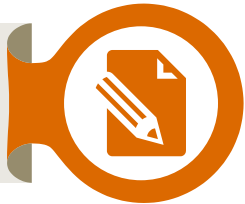
Detailed Findings



Accounts Receivable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P1 15/16
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	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P1 15/16
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 10/20 debts, the debt was not chased every 30 days in line with the debt recovery policy. For 9/10 exceptions, this was due to no chasing letters being sent in September and October 2017. For 1/20 debts, the debt had not been chased due to a system error that failed to identify that this item required chasing. <p>Management response:</p> <p>We have discussed with the line manager how he can effectively supervise the team to ensure these monthly routines are followed. A monthly check list will be implemented to monitor monthly activities including sending of statements and reminders.</p> <p>Responsibility for action:</p> <p>Julian Rigby (Head of Financial Processing)</p>	●	●	●	●

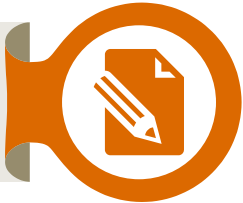
Detailed Findings



Accounts Receivable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
AR4 Student debt: reminder letters are sent in respect of overdue fees on a monthly basis in line with policy.	●	<ul style="list-style-type: none"> 3/25 student debts had not been chased in accordance with policy. For one debt, there had been no activity since June 2014. 1/25 student debts had been written off by the debt collection agency, but there was no audit trail retained to evidence that this had been authorised by an appropriate LSBU staff member. <p>Management response:</p> <p>A number of actions should have taken place in these cases. Some of these issues will be addressed through the monthly check list described in AR3. We will also discuss with our external debt collection agency how management can monitor our team's response to queries raised by them, including requests to close accounts.</p> <p>Responsibility for action:</p> <p>Julian Rigby (Head of Financial Processing)</p>	●	●	●	●

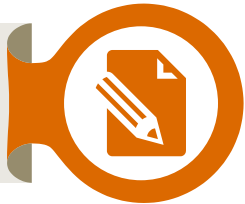
Detailed Findings



Accounts Receivable

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●		●	●	●	●

AR3: Debtor escalation
Control Design

4

Page 14

Finding rating

Rating	Low
---------------	------------

Findings

Reminder letters are currently sent to debtors 30, 60 and 90 days following the invoice issue date in respect of invoiced debt. There is no proactive action for debt recovery after the 90 day chasing letter is sent. As a result there are currently outstanding debts that are over 5 years old.

Implications

There is a risk that debts are not being collected on a timely basis and income is not being maximised.

There is also a risk that staff time is not being utilised effectively due to the resource commitment of chasing long-outstanding debts.

Agreed action

A process for escalating long-outstanding debts is in place, however this is not currently formalised. We will update our internal policies to clarify the escalation process.

Responsible person/title:

Natalie Ferer, Financial Controller

Target date:

28/02/2018

Reference number:

4

AR4: Write-off of student debt
Control Design

5

Page 115

Finding rating

Rating Low

Findings

There are several debts of large value that have been written off by the 3rd party debt collector without evidence of approval by an appropriate LSBU staff member. An audit trail of the write-off approval should be retained.

Implications

The debt collection agency may not be following the LSBU policy for debt recovery. This could mean that debts are written off prematurely.

Agreed action

We will put in place a monthly Accounts Receivable checklist and this will include recommendations for write off of debts to include both STA and in-house debt.

Responsible person/title:

Natalie Ferer, Financial Controller

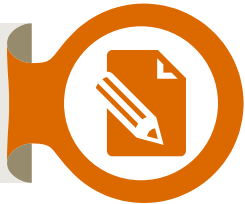
Target date:

31/03/2018

Reference number:

5

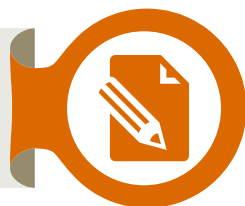
Detailed Findings



Cash

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●	●	●	●
C2	●	Cash deposits made by Loomis are reconciled to records of cash takings on a daily basis.	●	●	●	●

Detailed Findings



Cash

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●		●	●	●	●

C3: KX user access
Control Design

6

Page 18

Finding rating

Rating

Medium

Findings

Access rights are granted to individuals without documented approval from their line manager.

Implications

Inappropriate access to the KX system may be granted to employees.

Agreed action

A new user form will be put in place which will detail access required and new users will be required to complete the form and arrange for it to be authorised before being set up on KX.

Responsible person/title:

Natalie Ferer, Financial Controller

Sacha Marshall-Ocana, Head of Student Accommodation

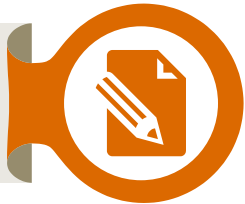
Target date:

31/01/2018

Reference number:

6

Detailed Findings



General Ledger

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
GL1 Journals must be authorised, with supporting documentation, prior to being posted on the system.	●	<ul style="list-style-type: none"> For 1/25 journals, there was no supporting documentation attached when the journal was posted. <p>Management response: Documentation should have been attached. A sample of journals are now being checked each month and cases of non compliance will be followed up with the staff posting those journals.</p> <p>Responsibility for action: Rebecca Warren (Financial Accountant) /Loretta Audu (Financial Accountant)</p>	●	●	●	●
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.	●		●	●	●	●

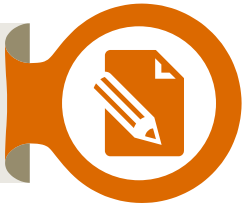
Detailed Findings

General Ledger



Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
GL4 Balance sheet control accounts are cleared or reconciled on a monthly basis.	●	<ul style="list-style-type: none"> 1/20 reconciliations was prepared 76 days after the end of the financial period to which it relates. All other reconciliations were prepared within one month of the period end. 6/20 reconciliations were authorised 82 days after the end of the financial period to which they related. All other reconciliations were reviewed within one month of the period end. 2/20 reconciliations contained a historic balance that had not been cleared since April 2017. <p>Management response: The delay in reviewing was due to the year end and the implementation of the new monthly checklist. Since November 2017 all reconciliations are reviewed within 15 working days.</p> <p>Responsibility for action: Natalie Ferer, Financial Controller</p>	●	●	●	●

Detailed Findings



General Ledger

Key Control	P2 17/18	Details on exceptions	Prior period exceptions			
			P1 17/18	P2 16/17	P1 16/17	P2 15/16
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.	●		●	●	●	●

GL1: Retrospective Approval of Journals
Control Design

Page 122

7

Finding rating

Rating

Medium Risk

Findings

Manual journals are approved retrospectively in batches. We would expect journals to be approved prior to posting in Agresso.

Implications

- Invalid, incomplete or inaccurate journals may be posted in the system.
- Fraudulent entries may not be detected.

Action plan

A new journal process is being finalised and put in place. The new process will require the majority of journals to be authorised before posting. Some journals, for example transfers between cost centres and source codes will still be approved retrospectively by the Financial Controller but the volume will be low, making it easier to review and address matters as they arise.

Responsible person/title:

Natalie Ferer, Financial Controller

Target date:

28/02/2018

Reference number:

7



**Appendix A: Basis of our
classifications**

**Appendix B: Terms of
reference**

**Appendix C: Limitations
and responsibilities**

Appendices

Page 123

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

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

2017/18

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

Page 126

Background and audit objectives



This review is being undertaken as part of the 2017/18 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.

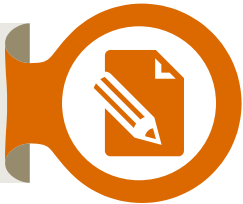
Our work touches upon the following areas that form part of our annual report to Audit Committee:

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

x = area of primary focus

x = possible area of secondary focus

Audit scope and approach (1 of 4)

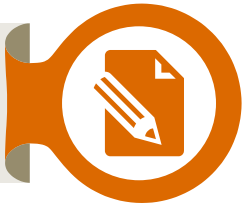


Scope

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)

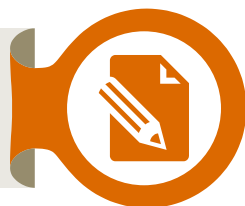


Scope

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 2017/18:

- Phase 1: January 2017 – July 2017
- Phase 2: August 2017 – December 2017



Internal audit team



Internal audit team

Name	Role	Contact details
Justin Martin	Head of Internal Audit	0207 212 4269 justin.f.martin@pwc.com
Lucy Gresswell	Engagement Manager	07718 098 321 lucy.j.gresswell@pwc.com
Janak Savjani	Engagement Supervisor	07802 660 974 janak.j.savjani@pwc.com
Josh Thomas	Continuous Auditing Technician	07718 978 628 joshua.thomas@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
John Baker	Corporate and Business Planning Manager	0207 815 6003 j.baker@lsbu.ac.uk	Review draft report Review and approve final report
Natalie Ferer	Financial Controller	0207 815 6316 ferern@lsbu.ac.uk	Hold initial scoping meeting
Markos Koumaditis	Deputy Director of HR Business Services	markos.koumaditis@lsbu.ac.uk	Review and meet to discuss issues arising and develop management responses and action plan
Victoria Mahoo	Interim Payroll Manager	mahoov@lsbu.ac.uk	Audit contact
Dave Lee	HR Systems & Analytics Manager	leed10@lsbu.ac.uk	Audit contact
Leo Kalzula	HR Recruitment Manager	kaluzal@lsbu.ac.uk	Audit contact
Norda Graham	Payroll Clerk	grahamn4@lsbu.ac.uk	Audit contact
Wayne Brown	Procurement Administrator	brownw@lsbu.ac.uk	Audit contact
Maureen Stanislaus	Payments Team Leader	stanism@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
Vic Van Rensburg	Income Team Leader	vanrensv@lsbu.ac.uk	Audit contact
Judy Robson	Accounts Clerk	robsonj2@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
Emily Parker	Procurement Services Operations Manager	parkere7@lsbu.ac.uk	Audit contact
Ravi Mistry	Financial Systems Manager	mistryrm@lsbu.ac.uk	Audit contact
Rebecca Warren	Financial Accountant	warrenra@lsbu.ac.uk	Audit contact
Sally Black	Financial Accountant	black6@lsbu.ac.uk	Audit contact



Timetable



Timetable

	Phase 1	Phase 2
Fieldwork start	14/08/2017	08/01/2018
Fieldwork completed	25/08/2017	19/01/2018
Draft report to client	01/09/2017	02/02/2018
Response from client	08/09/2017	16/02/2018
Final report to client	15/09/2017	23/02/2018

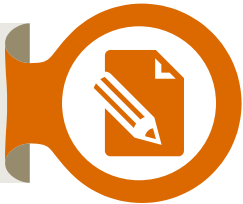
Agreed timescales are subject to the following assumptions:

- 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 LSBU 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, LSBU 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



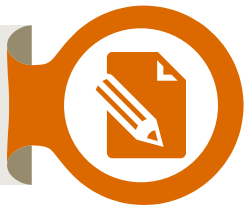
Based upon our understanding of the financial systems in place at LSBU and in discussion with management, we have agreed that the operating effectiveness of the following controls will be considered. These have been mapped to the key risks identified as in scope above.

Payroll

Key Contacts: Dave Lee (listings for P1, P2 and P6), Leo Kalzula (P1, P2, P6) Victoria Mahoo (P3 – P5, P8) and Norda Graham (P7 and P9)

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 documentation, including evidence of line manager approval, is 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; • 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: Ravi Mistry (listings for AP2 and AP3), Wayne Brown (AP1 and AP5) and Maureen Stanislaus (AP2 – AP4 and AP6)

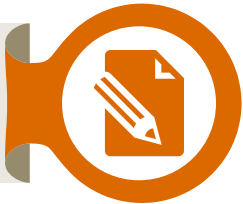
Key risk	Key Control	Reference
Invalid suppliers, or supplier standing data, is maintained leading to inaccurate or fraudulent payments	Authorised documentation must be received prior to the creating a new or amending a supplier record.	AP1
Payments are made for goods and services which have not been 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	Weekly 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

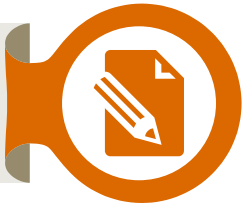


Accounts Receivable

Key Contacts: 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 (C1 – C3) and Judy Robson (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 and Sally Black (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/ reconciled and reviewed on a monthly basis.	GL3
	Balance sheet control accounts are cleared/ reconciled and reviewed 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 16/10/2017. 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 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.

© 2018 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

Paper title:	Internal Audit Report on IT Risk diagnostic & benchmarking exercise, with related Action Plan.
Board/Committee	Audit Committee
Date of meeting:	8 February 2017
Author:	PriceWaterhouse Coopers – audit report David Mead, Director of Academic Related Resources – action plan
Executive:	Ian Mehrtens – Chief Operating Officer
Purpose:	For Information; to provide Committee with the report on the risk, and the related action plan
Which aspect of the Corporate Strategy will this help to deliver?	Effective provision of IT services enables activity across the entire organisation, but relates particularly to goal 8 – Resources & Infrastructure.
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report and its findings

Executive Summary

There is no formal report classification for this report, which was conducted in order to establish a baseline understanding of the IT risk environment and maturity of internal controls across the LSBU IT landscape, utilising PwC’s risk diagnostic framework which enables benchmarking against industry peers.

The report presents a view of the maturity of controls in seven areas, and provides a context in which further developments or reviews could occur. The report identified one area in the second quartile: Information Security, and two areas as being in the bottom quartile, IT Operations and IT Governance, with three areas highlighted as high risk in the next steps suggestions in section 1d.

Academic Related Resources have produced the attached action plan in response to this report, which is provided to demonstrate progress made in response to the findings.

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

This page is intentionally left blank

IT Risk Diagnostic

London South Bank University

October 2017

FINAL

Page 149

Contents

1. Executive summary

- a. *Scope and Approach*
- b. *Executive Summary*
- c. *Benchmark Overview*
- d. *Next Steps*

2. Benchmarking background

3. Observations and Benchmarks

- a. *Strategic Decision Making*
- b. *IT Governance*
- c. *IT Management*
- d. *Systems Quality*
- e. *Systems Support and Change*
- f. *IT Operations*
- g. *Information Security*



Executive Summary

Page 151

1

a. Scope and Approach

i. Scope

This review has been undertaken as part of the 2016/2017 internal audit programme, which has been approved by the University's Audit Committee. The review was performed during May/June 2017 and all findings relate to the control environment at that time.

The purpose of this review was to establish a baseline understanding of the IT risk environment and maturity of internal controls across the IT Audit landscape within London South Bank University. This was performed by carrying out a series of meetings and workshops with the IT management team, to understand the processes and controls in place across seven core IT areas. Management's subsequent self-assessment of controls maturity in the seven areas have been benchmarked against both "good practice" and a group of 30+ organisations which includes both public and private sector organisations.

The review presents a view of the maturity of controls in the following seven areas within the IT Audit landscape:

- IT Strategy;
- IT Governance;
- IT Management;
- System Quality;
- System Support & Change;
- IT Operations; and
- Information Security.

Our results should provide a helpful starting point to identify areas of IT risk that should be considered by the Management team and provide further insight for the Internal Audit plan for 2017/2018 and beyond.

ii. Approach

The review was performed in the following stages:

- Initial IT risk consultation - We engaged with key stakeholders to understand the University's IT landscape and identify business drivers for IT as well as key IT control owners.
- Formal IT risk assessment - Our IT risk assessment was performed utilising PwC's proprietary IT Risk Diagnostic (ITRD) tool and framework. The ITRD assessment consists of 7 IT focus areas, covering 36 Technology risk areas. Controls were assessed according to the impact and maturity levels identified through a series of workshops.
- Validation of IT risk diagnostic findings - We used the results of the IT risk questionnaire to develop a view of the University's IT risk landscape. This enabled us to benchmark the level of controls maturity across the 36 IT processes, against industry peers.
- Audit planning and scoping - We have then identified potential audit activities, grouped by the risk level and impact to the University.

b. Executive Summary

London South Bank University has a generally controlled IT function. Our benchmarking exercise has identified that the University has benchmarked typically in the third quartile against peer and similar sized organisations (see section 2 for details).

This has not been due to widespread absence of an IT control framework however and no single domain was found to be totally lacking in expected controls. The key theme that came out of the review was that efforts need to be made to formalise and update existing controls so that either their scope widens or they become more consistently executed. For example, periodic asset management checks are taken, but not in the context of an actual asset management policy driving ongoing behaviours.

We noted that IT are developing a number of initiatives to rectify certain areas of deficiency. For instance, the University have plans in place to increase their maturity in mapping interdependencies across IT systems and processes and have recently worked to improve training programmes for staff.

The primary objective of the review was to benchmark the IT control environment against peer organisations. As a result of this benchmarking exercise there is also an opportunity to highlight a number of areas that would benefit from review by internal audit in the short, medium and longer term. The key weaknesses areas, each considered as high risk, are as follows:

1. IT Governance

Although the University have a formalised IT Security policy in place, there are a number of other IT policies that have not been reviewed and updated. Additionally, the University does not have an up-to-date central repository where all IT policies are stored and periodically reviewed.

There are no IT service level agreements (SLAs) in place between IT and the wider University, as a result there is an absence of effective monitoring of the service provided by IT to ensure it is delivering value for money and supporting the University and its students.

2. Systems Support and Change

There are support teams in place for key components and systems however, there remains some single points of failure (key staff). Additionally, despite the launch of a training database, IT training is informal and infrequent. This may lead to loss or unavailability of knowledge and may result in IT's inability to effectively support the business.

The University have high level and low level designs in place for a number of key systems, however these have not been signed off and are now out of date. Without appropriate and up-to-date documentation in place system performance may degrade due to unrecorded and understood customisation that cannot be rolled back.

It was identified that for some systems all developers retain production access. The absence of access control mechanisms or access reviews around developer access to the production environment may lead to unapproved changes being implemented. This may result in systems instability and significant business disruption.

3. IT Operations

The University have large amounts of legacy hardware in place now unsupported by the vendor or requiring specialist (and expensive) knowledge to maintain and run. This increases the risk that, in the event of an incident, the University will be unable to provide effective support which may result in business disruption.

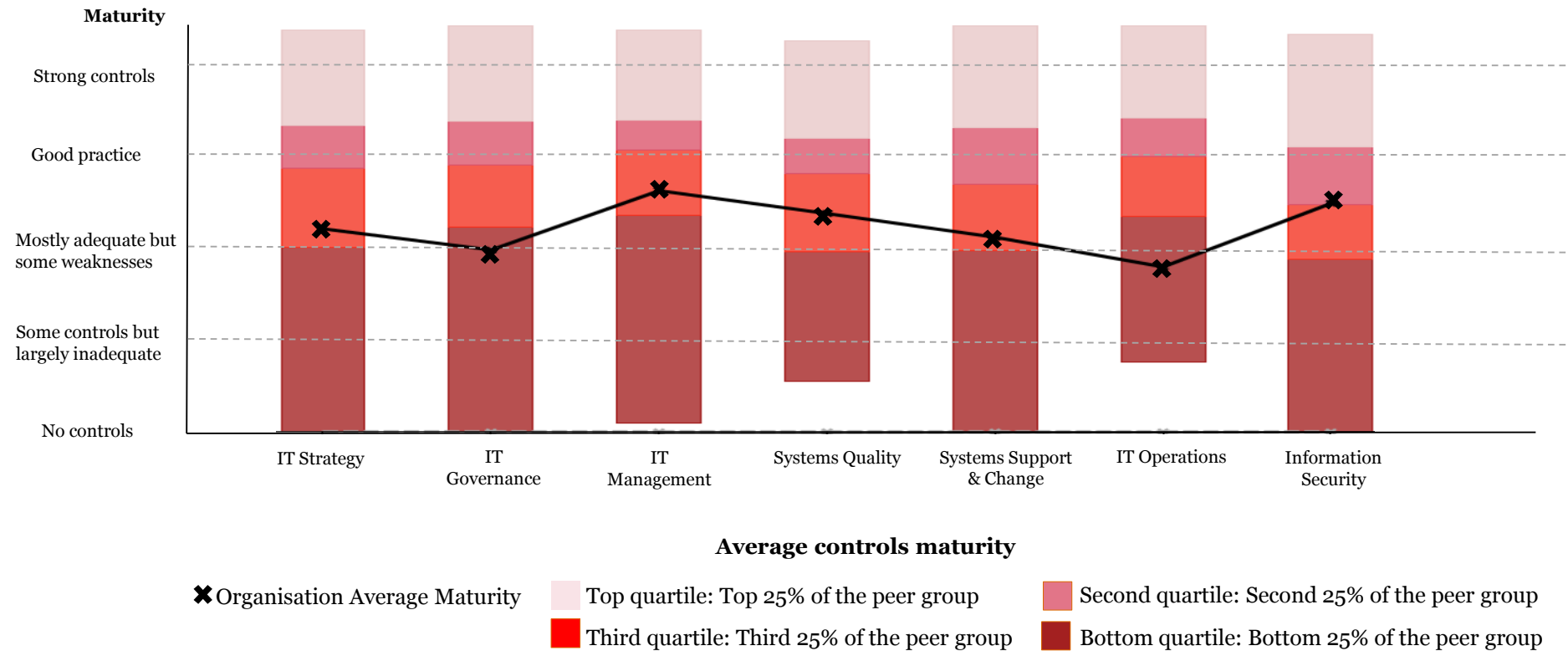
There are no formalised problem management and IT Business Continuity procedures in place. Additionally, the major incident management policy is not aligned to the University's Emergency Management Policy. The absence of formalised and effectively aligned policies may result in an inability to address business needs in case of a major outage.

There are disaster recovery (DR) arrangements in place for specific systems. However, DR plans have not been signed off by appropriate parties. The lack of appropriate IT DR testing may lead to an inability to restore services when needed, resulting in major outages or business disruption.

c. Benchmark Overview




The graph below summarises IT Management's self assessment of controls maturity across the seven areas of the IT Risk Diagnostic Review. Further detail is provided in each area within the conclusion section.

Page 154



d. Next Steps – Audit Planning

The table below sets out a summary of areas that may benefit from audit focus in 2017/18 and beyond. The proposed areas of audit focus are grouped by risk level with a short definition being given for each level.

	 High	 Medium	 Low
	Immediate action is recommended to address significant weaknesses in the system of internal controls which exposes the organisation to an unacceptable risk.	Action is recommended within agreed timescales, to address weaknesses in the system of internal control which increases organisational risk.	Action should be considered, although the current exposure to risk is unlikely to be significant. Action to be taken is at the discretion of the organisation.
	Should be considered included as part of FY 17/18 IT Audit plan.	Should be included as part of IT Audit plan in the next 2 to 3 years.	Should be considered its inclusion as part of IT Audit plan in the next 3 to 5 years.
	Areas to be considered <ul style="list-style-type: none"> • IT Governance (IT Governance) • Standardisation of IT/ Enterprise Architecture (Strategic Decision Making) • IT Disaster Recovery (IT Operations) 	Areas to be considered <ul style="list-style-type: none"> • IT Performance Management (IT Governance) • Information Classification (Information Security) • IT Knowledge Management (IT Systems support) 	Areas to be considered <ul style="list-style-type: none"> • Third Party Management (IT Management)

Benchmarking background

Page 156

2

Benchmarking background

The PwC IT risk diagnostic tool is used across our global client base creating hundreds of data sets against which to benchmark.

LSBU as a University is a unique organisation compared to many, but the nature of its information security risks are still common to those in other businesses/industries.

These include the risks arising from:

- Holding business critical information assets (such as exams and research data)
- Holding customer/student data
- Holding employee data

As result of these, on a judgemental basis, benchmarking has been applied against small/medium sized entities using the following industry groups within the tool: Education, Utilities, Local Government, Professional services, Telecommunications, Construction, Transportation, Information Technology, Leisure, Media.

Observations and Benchmarks

Page 158

3

a. Strategic Decision Making

Structure to align the IT Strategy and objectives to achieve the overall business strategy

 **Medium**
(overall risk presented by area)

Observations

- The University's IT Strategy was finalised in February 2017. The strategy was reviewed by the operation board, senior management and the wider business prior to finalisation to ensure it was aligned to the needs of wider stakeholders.
- Decision making across the IT organisation is supported by appropriate staff grades. However, not all IT and business stakeholders have been identified and roles and responsibilities are not captured in a formalised RACI matrix for IT services.
- The University does not have a formalised approach to drive innovation and there are no resources specifically assigned to proactively research new technology. Despite this both IT and business staff make a concerted effort to remain informed about emerging technologies and there are relationships in place with external vendors. A number of staff go to trade shows to research new technology.
- IT across the organisation has not been standardised to a high degree. In relation to enterprise architecture, interdependencies between systems, processes and risks have not been fully considered captured and understood. This is a known weakness by management and there are plans to address this in the future.
- The University has an Environmental Policy and a Power Usage Group Policy in place which is being followed by IT in an effort to be sustainable. This has created some good behaviour such as recycling equipment and saving power on desktops. The University have a sustainability team in place which monitor the University's power usage. However, management information is not effectively captured and, as such, monitoring is done on an ad hoc basis and not formally targeted at IT.

Risks

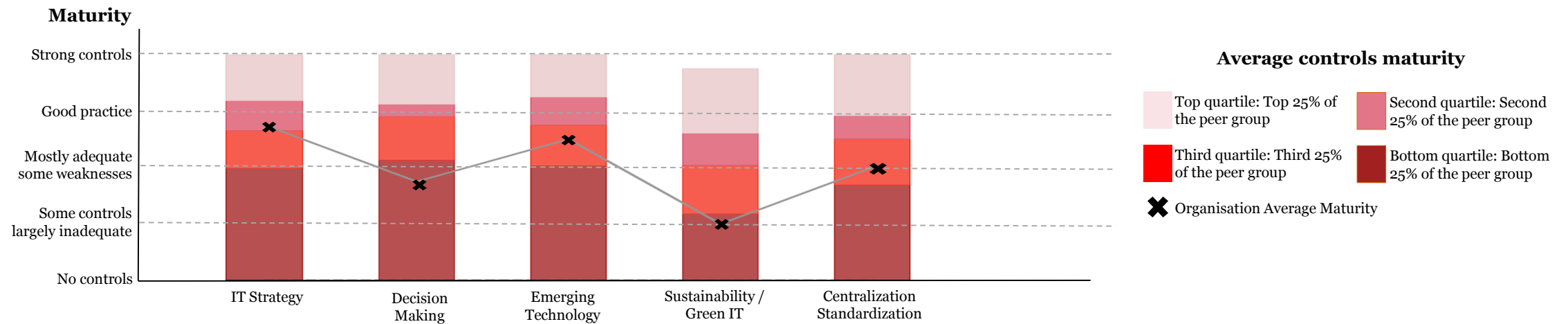
- The lack of defined responsibilities may lead to either delays in decision making or sub-optimal decision making, resulting in IT being unable to deliver on its strategic objectives.
- The absence of mapped interdependencies across people, processes and technology increases the risk that an issue with/or change to a particular IT component may adversely affect other systems, which may lead to severe disruption of IT services.
- The absence of consistent management information around sustainability may result in inconsistent/inaccurate reporting which could lead to a lack of awareness around the effectiveness of IT sustainability measures.

a. Strategic Decision Making

Structure to align the IT Strategy and objectives to achieve the overall business strategy
(continued)

● Medium

Page 160



Conclusions

Responsibilities regarding the decision making and delivery of IT services are not clear and a formalised RACI matrix is not in place. The absence of clearly defined and understood roles and responsibilities may result in delays on critical decisions leading to business disruption or failure to enforce decisions made. This may present an opportunity for Internal Audit to review the governance and decision making process to identify potential gaps.

The University's IT services are not standardised. The organisation do not have a holistic approach of system processes, risks have not been strategically considered and, as such, interdependencies have not been mapped. Senior management have recognised their deficiencies and an initiative is planned to increase the University's level of maturity here.

The University consider green IT in their decision making process and a sustainability team is in place with the remit of monitoring power usage. However, the University do not effectively capture management information and, as a result, monitoring is done on an ad hoc basis.

b. IT Governance

Framework to support effective decision making between Corporate IT and the decentralised structure of the group



High

Observations

- There are a number of IT governance forums and boards, such as the ICT Board, Strategy Board and Senior Management Team Board, which meet every week or fortnightly to manage, control and monitor IT. A weekly forum has also recently been established between Information Transformation and IT services with the aim of ensuring communication channels are in place between IT teams to prevent IT staff working in silos.
- Meeting minutes are produced for senior IT management meetings but communication of initiatives and change is not always forthcoming. For instance, it was acknowledged during the workshop that not all IT staff were aware that the University are in the process of assessing the future data centre strategy.
- The University does not have an up to date central repository where all IT policies are stored and a policy review process has not been designed to ensure IT policies are up to date and aligned to industry good practice. There are a number of policies that have not been reviewed and updated, whilst other policies have been updated but not published and communicated. Additionally, in the absence of clear policy ownership, policies are not signed off and effectively enforced.
- The University have an Infrastructure Board in place, which decides where IT investment should be allocated. Additionally, a steering committee will oversee the delivery of all major projects over a certain financial threshold.
- A formalised risk management framework is not in place. IT risk owners are not defined and risks are not considered for all operating areas. It was noted that risks are evaluated by analysing likelihood and impact, however the criteria of assessing risks are not effectively understood. Additionally, quarterly or other periodic assessments of risks or any formalised risk management training does not takes place.
- The IT function does not have defined Service Level Agreements (SLAs) in place with the business, which prohibits comprehensive monitoring of IT performance. It should be noted that service objectives are in place but were not explicitly agreed with the business and, as such, if objectives are not met, no resulting action is taken. Since February 2017, the University has begun to monitor performance of the service desk, the network and bandwidth across its site as well as uptime of equipment.

Risks

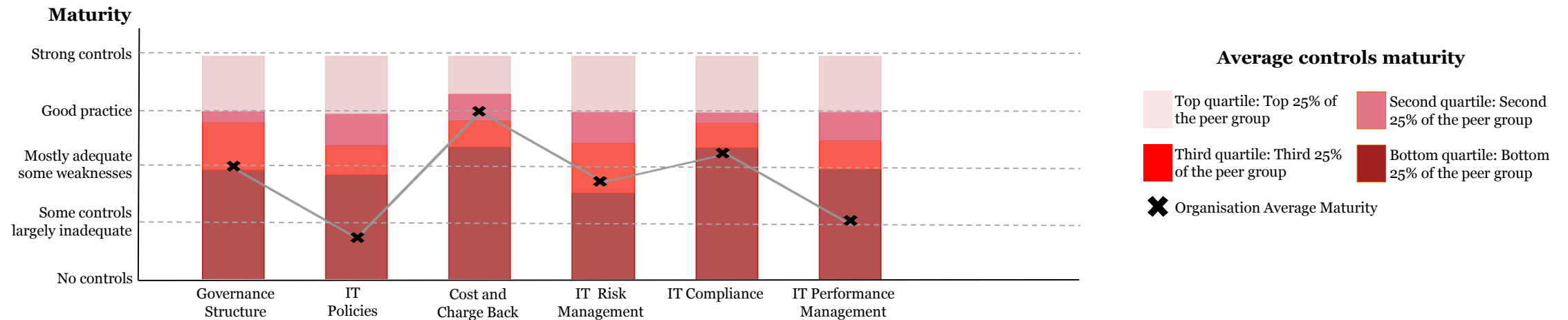
- Responsibilities and accountabilities may not be known and understood across the organisation, resulting in disruption to the University's services in case of an incident.
- The absence of effective communication of identified actions from governance forums may lead to a lack of clarity in delivering services. As a result, business needs might not be addressed effectively or in a timely manner.
- The absence of up-to-date IT policies increases the risk of ineffective mechanisms for managing information security activities, resulting in security breaches, major outages and /or reputational issues.
- Insufficient assessment and monitoring of IT risks can result in inadequate process controls being implemented to mitigate disruption to the IT applications and infrastructure that support the University's services.
- The absence of formalised SLAs may result in a misalignment of expectations between IT and the business, resulting in a degradation of IT service quality.

b. IT Governance

Framework to support effective decision making between Corporate IT and the decentralised structure of the group (continued)

● High

Page 162



Conclusions

Governance controls and processes across IT carry some significant weaknesses that need to be addressed to ensure ongoing optimum return on investment and the delivery against IT strategy. It is suggested that these areas be looked at further by internal audit in the future.

These include:

- Clarity around roles with the IT team and associated accountabilities and responsibilities;
- Up-to-date, agreed and understood policy framework;
- Risk management controls including agreed thresholds, mitigations and ownership; and
- SLA's defined and agreed with the business against which performance can be monitored.

c. IT Management

IT manage activities to meet business requirements and demonstrate business value



Low

Observations

- IT Management have some limited processes in place to collate management information and produce monthly reports; these relate to IT Change Management and revenue/budgets for projects.
- As at July 2017, IT had 25 live projects ongoing and an emerging portfolio of 90 projects over the next 3 years. The University adopted a pipeline approach in 2015 to manage upcoming projects, however whilst the business impact is captured for each project, benefits are not quantified. All projects have a technical project manager to oversee the day to day running for each project and an overall business owner who authorises proposals and take responsibility for the output of the project.
- There is a clear governance structure to manage projects during their lifecycle. Fortnightly meetings are in place to review any issues with individual projects. If they are unable to be rectified, issues will then be taken to the monthly project board to be reviewed by senior management. Monthly reporting of project milestones and dependencies is in place and issues are tracked on a dashboard mechanism.
- To support the management of staff there are standard job descriptions outlining scope of work/roles and reporting responsibilities in place. There is a formalised process for managing and hiring IT resources and yearly training is in place which focuses on facilitating personal growth and development of IT skills (although this is not system specific training).
- The University have an applications register in place, which holds roughly 400 applications. Although 20 systems are out of vendor support, no critical systems (as defined by business continuity) are out of support.
- The University have a number of third party suppliers in place. Key third parties (tendered since 2015) all have clear SLAs in place and procurement actively works with IT to ensure that SLAs are appropriate for the business and each undergoes a robust review process. A contract database exists with contract and category managers with clearly owned relationships in procurement or IT are in place.
- The University do not have a software licensing policy in place, however related procedures are outlined within the IT acceptable usage policy. Controls exist around who can buy software and the business is required to approve the purchase of software for a non-standard build.
- The University has developed an asset management policy, but it is in the process of being signed off. A VMware and full server asset inventory is in place and, over the past three months, the University has also undertaken a full network audit. Moreover, an automated tool, System Centre Configuration Manager (SCCM), is in place to monitor hardware inventory.

Risks

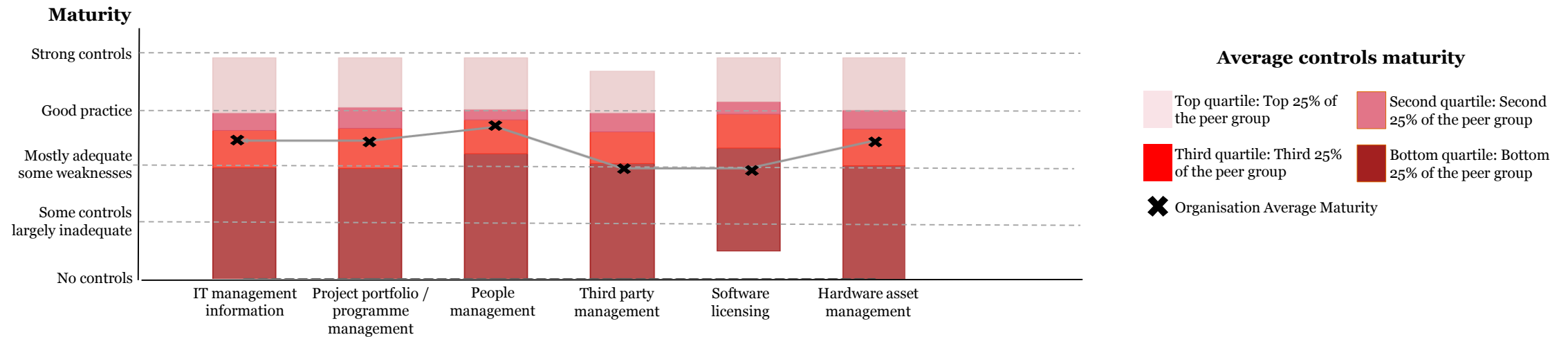
- The absence of a formalised and signed off asset management policy increases the risk that the degree of compliance may deteriorate and inappropriate or incorrect actions may be taken, increasing the likelihood of disruption to services.

c. IT Management

IT manage activities to meet business requirements and demonstrate business value (continued)

● Low

Page 164



Conclusions

Efforts to manage third parties and monitor delivery aligned to SLA's and expected behaviours has improved since 2015, but longer term legacy providers may not still be subject to these control mechanisms.

The absence of asset and software management polices means that although there are steps taken to minimise loss in these areas, the ongoing term activities of staff may remain uncontrolled due to expected actions/behaviours not being articulated and subsequent financial loss minimised.

d. Systems Quality

Effectiveness of systems to support the business and IT's ability to support future business initiatives

 **Medium**

Observations

- In general, systems are considered by the IT management team to be effective in meeting current business needs, for example the HR and payroll systems. However, staff are unhappy with some key third party systems from particular suppliers, expressing their dissatisfaction with system functionality.
- The University launched a data warehouse in April 2017, with the aim of collating data from multiple sources into a single repository for analysis. A business intelligence (BI) programme and strategy are not in place and, as such, BI is not consistent. For instance, BI for student returns is robust and reports are produced for clearing, admission and marketing. However, ad hoc reports are produced for other systems.
- A Data Assurance Group is in place, which is made up of data stewards with the remit of providing effective data governance. The group is scheduled to meet twice a year and data stewards are expected to meet quarterly.
- An End User Computing Policy is not in place and there is a large amount of shadow IT expenditure at the University. Staff are able to buy hardware for their own purposes and there are local controls at network and desktop level to stop unauthorised software installations.
- The majority of projects are delivered successfully. However, in the absence of a formalised mechanism to track risks and issues, lessons learnt are performed on an ad hoc basis and not formally shared. Since December 2016, the University has made a concerted effort to improve handover from development to production support to minimise go-live issue.
- The University does not have a formalised project risk management framework in place, however a traffic light system to accept risks is in operation. Projects do not have their own risk register and an overarching risk register encapsulating all projects is not in place. As such, interdependencies between risks and issues between projects are not mapped.
- The University have consistent procedures in place for the acquisition of new technology. When new technology is procured, a business case needs to be presented alongside its proposed costings. During the review process, a comparison will be undertaken to understand the financial differences between the development and purchase of new technology.

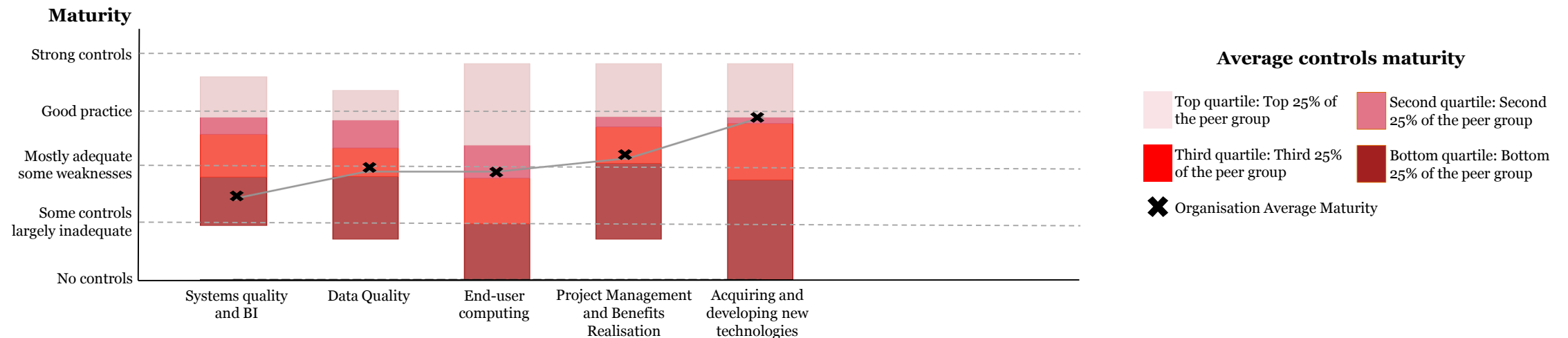
Risks

- The absence of robust BI for all key systems may lead to an inability of to produce adequate reporting resulting in ineffective decisions being made by senior management and consequently financial losses or poor business performance.
- The failure to effectively capture and identify project related risks and to design appropriate mitigating controls in a formalised project risk register increases the risk of financial, operational, regulatory and reputational impact.
- The absence of formalised and widely shared lessons learned processes increases the risk of a repeat of issues that could have been prevented.

d. Systems Quality

Effectiveness of systems to support the business and IT's ability to support future business initiatives (continued)

● **Medium**



Page 166

Conclusions

In a joint venture between IT and the business, the University launched a data warehouse in April 2017 with the aim of have a centralised record of all data. While BI for student returns is robust and reports are produced for clearing, admission and marketing, BI is not consistent for all systems and only ad hoc reports are produced for some systems. As a result, the University is inhibited in its process of having robust data which limits senior management's ability to make informed decisions.

The University do not have an End User Computing Policy and limited control mechanisms are in place to manage shadow IT expenditure. As such, staff can purchase externally hosted software and hardware without being questioned.

The absence of a formalised process to identify, capture and document risks highlights the lack of controls maturity in risk management. As such, we recommend the University establishes a formalised risk management framework to ensure inadequate process controls are not implemented which could have cause severe disruption to University services.

e. Systems Support and Change

Effectiveness of systems to support the business and IT's ability to support future business initiatives



High

Observations

- The IT function tries to ensure systems have dedicated support resources. The University have mostly internal support teams in place apart from networking and security services, which are managed externally. IT Management consider the infrastructure support teams to be under resourced and there are single points of failure in terms of support across the application portfolio.
- IT training on systems is currently informal and infrequent. For instance, the University has had a QL tool in operation for ten years but staff were last trained on the tool nine years ago. As a result, knowledge is outdated. The University launched a new training database which is up to date with new mandatory programmes however training remains informal and infrequent.
- There are architectural designs in place for the majority of core critical infrastructure and both high level designs (HLDs) and low level designs (LLDs) are in place for a number of key systems. However, these have not been signed off and are about a year out of date and no formal process for devising enterprise architecture is in place due to the lack of an architect.
- A formally defined and approved change management process is in place. Low risk changes are authorised by line managers and changes that have not been authorised by line managers are taken to CAB. These are required to have completed roll back plans and impact assessment plans in place. The CAB is attended by both technical authorities and business owners to assess the change request and once approved, changes are scheduled accordingly. If the change requester is not present at CAB, the change will not be approved.
- A system baseline is not in place to understand if changes have previously taken place and no routine configuration checks are undertaken.
- The University use version coding for all changes. They are currently working towards developing formalised coding standards but no documentation has been ratified. Additionally, formal end to end testing is not undertaken due to resourcing and funding issues only User Acceptance Testing (UAT) is obtained and most projects will not proceed to production without passing this.
- The University have five developers in place. Unlimited access to all systems is not provisioned, however there are some systems where all developers retain access to production environment. When developers leave the team, their access is manually removed. Due to the small nature of the team, access reviews do not take place.

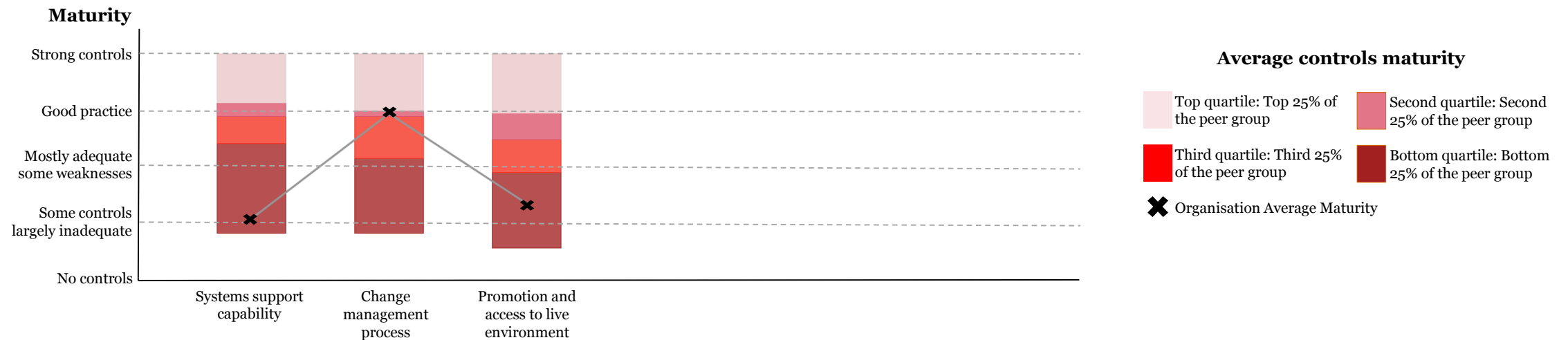
Risks

- The existence of skills shortages may lead to knowledge gaps and consequently may result in an inability of IT to support the business resulting in prolonged outages and business disruption.
- The lack of user education will lead to inefficiencies in the work force as employees are unsure of the best channels to seek support or they may use systems without the appropriate knowledge. This could result in major outages or a low quality of service.
- The lack of robust end-to-end testing could result in critical issues not being tracked and tested, increasing the likelihood of problems during release and implementation.
- In the absence of up-to-date architectural documentation sub-optimum investment decisions may be made where they contradict or do not enhance existing IT systems and processes.
- The absence of access controls mechanisms and processes regarding developer access to the production environment may lead to unapproved changes being implemented resulting in significant business disruption and financial or reputational losses.

e. Systems Support and Change

Effectiveness of systems to support the business and IT's ability to support future business initiatives (continued)

High



Page 168

Conclusions

The University's IT function ensures key systems have a dedicated support team in place, however IT management believe infrastructure support teams are understaffed. The existence of single points of failure within the support teams increases the risk of individuals being unable to access key knowledge when required, which may result in prolonged outages and business disruption.

The University have ad hoc training in place for IT staff. Although they have recognised their deficiencies in this area by initiating a new training database with mandatory programmes in place, training remains informal. This increases the risk of IT staff not being able to effectively support the business which may result in prolonged IT disruption.

The University have a formalised change management procedure in place. However, due to lack of budget and resources, formalised end-to-end testing procedures are not in place. The absence of robust testing increases the likelihood of problems during release and implementation of changes.

f. IT Operations

Ability to support the business as usual environment



High

Observations

- The data centre has access controls in place. The University has perimeter guards, controls and CCTV. There are instances when unauthorised individuals enter the IT area but data centre access is restricted. User access into the main office is logged as visitors have to sign a book and are issued with a pass.
- A number of computer laboratories are secured using physical keys, whereas others have been equipped with modern card readers. Communication cabinets use both types of physical control. For out of hours access, a code and key pass with appropriate access authorisation is required but codes are not frequently changed.
- The University has a large portion of old hardware on the server side. Staff do not feel they receive the level of support required to run the infrastructure effectively and they have experienced a number of issues with the underlying hardware.
- The University has formalised documentation for batch processing and have role based accounts, which enables staff to investigate issues where necessary. The infrastructure team run batch processes and receive daily notifications on jobs. It was felt by management that batches are running increasingly smoothly and, in case of failure, analysis is undertaken.
- The University do not have a documented problem management process in place. However, during discussions with senior management, it was noted they are in the process of developing formalised problem management procedures.
- A major incident policy is in place. However, it is not aligned with the University's Emergency Management policy. There are discrepancies between points of contact and the incident policy does not outline delegated individuals who should be contacted in the event of unavailability of primary contacts. It should be noted that root cause analysis is undertaken for major incidents. The University have recognised their policy deficiencies and are currently in the process of formalising service management procedures.
- The University have Disaster Recovery (DR) plans in place for specific systems, however they have not been approved and signed off by the business. They do not undertake DR tests for major systems and, as such, staff are unaware of the system downtime that would occur in the event of a disaster situation.
- A formalised University wide Business Continuity Plan (BCP) is in place, which includes information on duty managers and roles and responsibilities. IT does not however have a specific BCP plan and, in the event of an emergency, IT may not know the correct procedure to undertake.

Risks

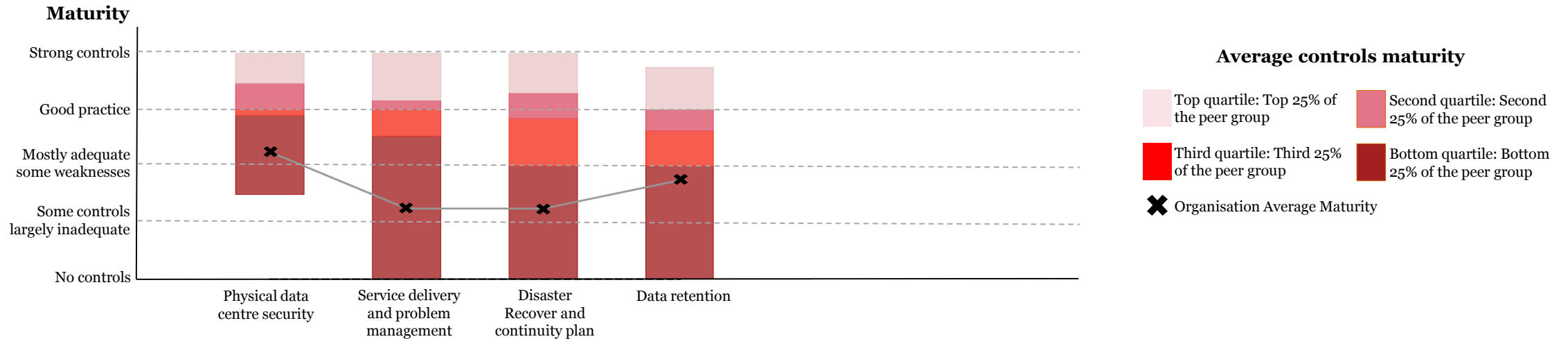
- The high volume of legacy hardware increases the risk that effective support is not provided for the systems from vendors or staff, which may result in major outages or business disruption.
- The absence of DR/BCP testing increases the risk of an inability to restore services in a timely manner which may result in major outages or business disruption.
- The absence of problem management procedures increases the risk that issues will not be mitigated in a timely manner, which may result in continued disruption to IT services.

f. IT Operations

Ability to support the business as usual environment (continued)

High

Page 170



Conclusions

The University has infrastructure in place enabling a high level of physical security. However, staff awareness needs to be improved as instances have been noted where credentials have not been effectively checked and computer laboratory rooms being left unlocked.

The major incident policy is not aligned with the University's Emergency Management policy, with points of contact not managing. This increase the risk that staff will be unable to respond to issues in a timely manner, which may have detrimental data, financial and reputational impacts for the University.

DR plans are in place which have not been formalised by the business and testing has not taken place for major systems. As such, if a disaster were to occur, staff would not know system downtime and would not be able to communicate the extent of potential losses of IT services. This area should be considered for inclusion in the IT audit plan to assess the appropriateness of the IT DR function in place and whether they can ensure an end-to-end recovery.

g. Information Security

Controls to ensure the confidentiality, integrity and availability of business critical information

 **Medium**

Observations

- There is an Information Security Policy in place which has been approved and signed off by senior management. The policy is well understood and has been aligned with counter terrorism requirements and the Data Protection Act.
- The University currently has a Head of Information Security, however there are resourcing gaps for other information security related roles and a security team is not in place. The University are reliant on operational teams to provide reports on information security. In the absence of a formalised team, actions to address information security actions are often not taken in a timely manner. Additionally, a Security Engineer is not in place so antivirus is managed on an ad hoc basis.
- Since March 2017, a mandatory staff awareness programme has been in place, which has to be completed within 6 months. Contractors on fixed term contracts are required to undertake the awareness programme.
- The University has user access controls in place. Single sign on and a system directory is used for all systems. Access provisioning is performed on a roll based system and access is given as required. Additional elevated access is provided on an exception basis.
- The University has a formal leavers process in place. Users are required to complete a form, which requires approval and signoff from HR, once completed all access is usually revoked by IT within 24 hours. It should be noted that user access reviews are not periodically performed.
- An intrusion detection system (IDS) system is in place. System admin rights are restricted based on role and reviewed by the Head of Information Security on a quarterly basis. Logs are extracted and reported for most windows systems, servers and firewalls. Third party providers undertake a manual review of the logs. The University is not involved in the review process but do receive a ticket if an issue arises. The University do not have formal escalation procedures in place. However, root cause analysis is undertaken for major incidents.
- The University have a formal process in place to identify cyber threats. An automated vulnerability scan takes place on a weekly basis and scans over all external facing systems but not all key systems. Automatic reports are generated for the Head of Information Security, which outlines output from the vulnerability scans. An internal vulnerability management process is not in place and penetration testing is not performed. Anti spyware software is not enabled on any student machines but there have been no significant virus outbreaks in the past 2 years. To note, the University were affected as part of the 'Wanna Cry' virus in May 2017, however only 14 out of 4700 devices were infected and all issues were resolved within 24 hours.
- Information classification procedures are not in place. However, secure waste disposal takes place.

Risks

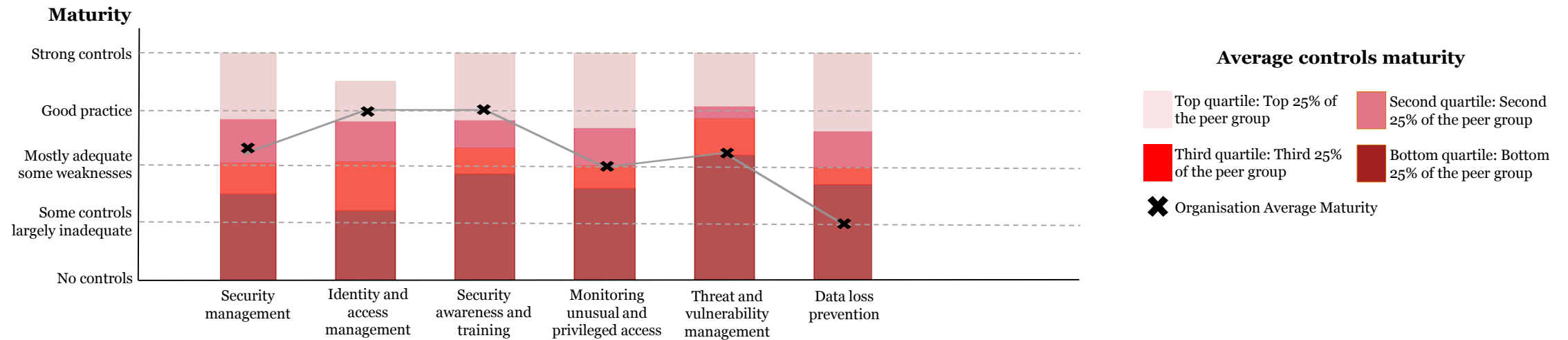
- The absence of an information security team may lead to an unavailability of knowledge/resource and may result in an inability for IT to successfully secure its data.
- In the absence of periodic access reviews, access to computing resources may not be revoked in a timely manner upon termination of employment, which increases the risk of malpractice from third parties, leading to potential financial, operational and reputational issues.
- The absence of document classification procedures increases the risk that during a document's lifecycle, sensitive information can be exposed to inappropriate personnel leading to reputational, financial, operational and or legal issues.

g. Information Security

Controls to ensure the confidentiality, integrity and availability of business critical information (continued)

● Medium

Page 172



Conclusions

The University have a Head of Information Security, however supporting security staff are not in place, in particular there is no role for a Security Engineer.

The absence of out of hours escalation protocol heightens the risk of issues not being detected and/or escalated in a timely manner, harming the University's services. This may pose an opportunity for the Internal Audit team to conduct a review on Cyber detection and response procedures to ensure that vulnerabilities and threats are managed appropriately.

Although the University waste is securely disposed, it was also acknowledged that formalised data classification procedures are not in place which may lead to data loss or the disclosure of confidential information. Therefore, a review could be carried out over the appropriateness of the classification scheme, monitoring mechanisms and any awareness activities.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

If you receive a request under Freedom of Information Legislation to disclose any information legislation to disclose any information we provided to you, you will consult with us promptly before any disclosure.

© 2017 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

1. Background

1.1. In June 2017 auditors PwC were commissioned to carry out a risk diagnostic of ICT Operations. The PwC report, attached separately, scores LSBU ICT risks based on evidence shown at the time of the diagnostic. The scoring is benchmarked with other organisations from Education, Utilities, Local Government, Professional Services, Telecommunications, Construction, Transportation, Information Technology, Leisure and Media.

1.2. The diagnosis looked at 7 areas and provided an overall risk score for each:

Area	Overall level of risk
IT Strategic decision making	Medium
IT Governance	High
IT Management	Low
System Quality	Medium
System Support & Change	High
IT Operations	High
Information Security	Medium

2. Action Plan and Governance

2.1. The diagnostic has provided a good baseline for us to review where we are focusing our resources. Since the diagnostic took place several actions have been put in place or are planned to take place. The table over the page sets out the actions that are in place or in the process of being implemented in response to the reports finding.

2.2. The implementation of the action plan is being co-ordinated by the internal ICT Senior Management Team meeting. All actions have a completion target date and as at January 2018 11 out of 24 actions were complete. Of the 11 actions complete, 7 were in the areas deemed to be 'high risk'. All actions are due to be completed within this year and the table over page sets out exactly when.

2.3. The overall maturity rating of the service placed LSBU ICT between 'Mostly adequate but some weaknesses' and 'Good practice evident'. Through undertaking the actions assigned we would expect to see this rating improve to between 'Good practice evident' and 'Strong controls in place'.

Ref	Area	Risk identified	Action	Action status
1	IT Strategic decision making- Medium Risk Area	The lack of defined responsibilities may lead to either delays in decision making or sub-optimal decision making, resulting in IT being unable to deliver on its strategic objectives	Governance Board now operational with terms of reference and attendees agreed- Board chaired by Exec member. We are currently creating a formal RACI template to ensure clarity of roles and responsibilities.	Complete To complete- March 17
2	IT Strategic decision making- Medium Risk Area	The absence of mapped interdependencies across people, processes and technology increases the risk that an issue with/or change to a particular IT component may adversely affect other systems, which may lead to severe disruption of IT services.	Work has been commissioned to document the systems and architecture.	To complete February 2018
3	IT Strategic decision making- Medium Risk Area	The absence of consistent management information around sustainability may result in inconsistent/inaccurate reporting which could lead to a lack of awareness around the effectiveness of IT sustainability measures.	Sustainability Management information dataset to be created.	To complete in June 2018
4	IT Governance- High Risk Area	Responsibilities and accountabilities may not be known and understood across the organisation, resulting in disruption to the University's services in case of an incident.	Major Incident plan has now been revised and updated and is regularly communicated.	Complete
5	IT Governance- High Risk Area	The absence of effective communication of identified actions from governance forums may lead to a lack of clarity in delivering services. As a result, business needs might not be addressed effectively or in a timely manner.	Bi-monthly meetings have been set up for sharing information as appropriate throughout all of ICT services.	Complete

Ref	Area	Risk identified	Action	Action status
6	IT Governance-High Risk Area	The absence of up-to-date IT policies increases the risk of ineffective mechanisms for managing information security activities, resulting in security breaches, major outages and /or reputational issues.	We have implemented several policies through the development of ITIL. This continues to mature and further policies added. A third party is also engaged to help with process documentation.	To reach level 3 ITIL maturity by July 18
7	IT Governance-High Risk Area	Insufficient assessment and monitoring of IT risks can result in inadequate process controls being implemented to mitigate disruption to the IT applications and infrastructure that support the University's services.	A risk and issues log is now integral to the weekly ICT SMT meeting.	Complete
8	IT Governance-High Risk Area	The absence of formalised SLAs may result in a misalignment of expectations between IT and the business, resulting in a degradation of IT service quality.	SLAs being developed. The data network access SLA is now in place. The Roadmap governance Board is now in place to manage expectations on project priorities and timescales.	To complete by September 2018
9	IT Management-Low Risk Area	The absence of a formalised and signed off asset management policy increases the risk that the degree of compliance may deteriorate and inappropriate or incorrect actions may be taken, increasing the likelihood of disruption to services.	Now signed off at Operations Board July 2017.	Complete
10	Systems Quality-Medium Risk Area	The absence of robust BI for all key systems may lead to an inability to produce adequate reporting resulting in ineffective decisions being made by senior management and consequently financial losses or poor business performance.	To review once we have output from systems and architecture work due to complete in March 2018	To complete in May 2018

Ref	Area	Risk identified	Action	Action status
11	Systems Quality-Medium Risk Area	The failure to effectively capture and identify project related risks and to design appropriate mitigating controls in a formalised project risk register increases the risk of financial, operational, regulatory and reputational impact.	Risk registers in place for all projects. Projects are reviewed weekly at the ICT SMT which includes looking at barriers and key risks.	Complete
12	Systems Support and Change	The absence of formalised and widely shared lessons learned processes increases the risk of a repeat of issues that could have been prevented.	Major Incident Reports cover lessons learnt. Projects now incorporate lessons learnt report upon closure.	Complete
13	Systems Support and Change – High Risk Area	The existence of skills shortages may lead to knowledge gaps and consequently may result in an inability of IT to support the business resulting in prolonged outages and business disruption.	Workforce plan being developed and staff are attending training courses as identified through appraisal and management meetings. Reducing the amount of technology we have to reduce the knowledge requirement across the service. Exploring support options for key systems where appropriate.	To complete in December 2018
14	Systems Support and Change – High Risk Area	The lack of user education will lead to inefficiencies in the work force as employees are unsure of the best channels to seek support or they may use systems without the appropriate knowledge. This could result in major outages or a low quality of service.	Digital Skills centre set up to support staff with the introduction of new systems. The recently approved asset policy sets out that all ICT purchases should be made centrally allowing better control. The new Data network SLA sets out all contact details.	Complete
15	Systems Support and Change – High Risk Area	The lack of robust end-to-end testing could result in critical issues not being tracked and tested, increasing the likelihood of problems during release and implementation.	New projects include testing requirements as part of the capital scope.	Complete

Ref	Area	Risk identified	Action	Action status
16	Systems Support and Change – High Risk Area	In the absence of up-to-date architectural documentation sub-optimum investment decisions may be made where they contradict or do not enhance existing IT systems and processes.	Work has been commissioned to document the systems and architecture.	To complete May 2018
17	Systems Support and Change – High Risk Area	The absence of access controls mechanisms and processes regarding developer access to the production environment may lead to unapproved changes being implemented resulting in significant business disruption and financial or reputational losses.	Change Advisory Board (CAB) meets weekly and a policy is in place that makes sure all change requests are approved through the board.	Complete
18	IT Operations- High Risk Area	The high volume of legacy hardware increases the risk that effective support is not provided for the systems from vendors or staff, which may result in major outages or business disruption.	Hardware replacement is under review and a priority on our technical roadmap.	To complete in July 2018
19	IT Operations- High Risk Area	The absence of DR/BCP testing increases the risk of an inability to restore services in a timely manner which may result in major outages or business disruption. The current infrastructure makes testing infeasible.	A more reliable and robust effective DR/BCP is dependent on the work being done on the infrastructure under the datacentre strategy.	To complete in December 2018
20	IT Operations- High Risk Area	The absence of problem management procedures increases the risk that issues will not be mitigated in a timely manner, which may result in continued disruption to IT services.	Problem Management procedure now developed and will be implemented over the next few months	To complete in Sept 2018
21	Information Security- Medium Risk Area	The absence of an information security team may lead to an unavailability of knowledge/resource and may result in an inability for IT to successfully secure its data.	The current capacity and capability is being reviewed.	Ongoing review

Ref	Area	Risk identified	Action	Action status
22	Information Security-Medium Risk Area	In the absence of periodic access reviews, access to computing resources may not be revoked in a timely manner upon termination of employment, which increases the risk of malpractice from third parties, leading to potential financial, operational and reputational issues.	We have scoped a role based access control project that is on our technology roadmap as a priority.	To complete by August 2018
23	Information Security-Medium Risk Area	The absence of document classification procedures increases the risk that during a document's lifecycle, sensitive information can be exposed to inappropriate personnel leading to reputational, financial, operational and or legal issues.	Training is provided to make staff aware of how to handle sensitive information. This is mandatory and constantly reviewed. To formally classify all documents we have would be an expensive undertaking so our approach is to mitigate the risk through training and awareness.	Complete

	CONFIDENTIAL
Paper title:	Corporate Risk Register
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	John Baker - Corporate & Business Planning Manager
Executive sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	For information; to provide Executive with the current corporate risk register ahead of Audit Committee, with the minutes from the Strategic Risk Review group for context.
Recommendation:	<p>The Committee is requested to note:</p> <ul style="list-style-type: none"> • the risks and their ratings, • the allocation of risks to corporate objectives

Executive Summary

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

Risks 14 and 518 have been reduced to medium likelihood following review by the January meeting of the Strategic Risk Review Group.

A revised format, as requested by the Board, is currently being drafted for review.

An overview of the updates and changes is provided in the middle column of the summary table on pages 2 - 3, with notes on overdue actions on the right, and the risks are grouped by the goals of the Corporate Strategy.

The Committee is requested to note:

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

This page is intentionally left blank

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

Date: 24th January 2018 **Author:** John Baker – Corporate & Business Planning Manager

Executive Lead: Richard Flatman – Chief Financial Officer

Impact	4 Critical <i>Corporate plan failure / removal of funding, degree award status, penalty / closure</i>			2: Revenue reduction if course portfolio, and related marketing activity, does not achieve Home UG recruitment targets (NL)
	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>	6: Management Information perceived as unreliable, doesn't triangulate (RF) 37: Affordability of Capital Expenditure investment plans (RF) 305: Data not used / maintained / processed securely (IM) 362: Low staff engagement (ME) 495: Higher Apprenticeships (PB) 519: Negative Curriculum Assessment (SW)	3: Increasing pensions deficit reduces flexibility (RF) 467: Progression rates don't rise (SW)	457: Anticipated international & EU student revenue unrealised (PI)
	2 Medium <i>failure to meet operational objectives of the University</i>	1: Capability to respond to change in policy or competitive landscape (DP) 517: Impact of EU Referendum result on regulation & market trends (DP) 494: Inconsistent delivery of Placement activity across the institution (SW)	14: Loss of NHS contract income (WT) 398: Academic programmes not engaged with technological and pedagogic developments (SW) 402: Unrealised research & enterprise £ growth (PI) 584: External incident compromises campus operations or access (ME) 518: Core student system inflexibility / failure (SW)	
	1 Low <i>little effect on operational objectives</i>			
		1 - Low	2 - Medium	3 - High
		<i>This risk is only likely in the long term</i>	<i>This risk may occur in the medium term.</i>	<i>The risk is likely to occur short term</i>
	Residual Likelihood			
Executive Risk Spread: VC – 2, DVC – 1, CFO – 3, PVC-S&E – 5, PVC-R&EE – 2, COO – 1, CMO -1, Dean Health – 1, ExD-HR – 2, US - 0				

Update Summary: Overview of changes since presentation at previous Operations Board, and overdue action progress updates:

Reference	Risk title	Completed Actions & Risk Changes	Overdue Action Progress Notes
Goal 1: Teaching & Learning: Ensuring teaching is highly applied, professionally accredited & linked to research & enterprise			
398 (SW)	Low engagement with tech or pedagogic developments		
467 (SW)	UG Progression rate doesn't rise	New action around MIKE data models and analysis.	
Goal 2: Student Experience: Seeing students as learning participants & encouraging and listening to the student voice.			
518 (SW)	Core Student System inflexibility / failure	Risk updated and likelihood reduced to 2: Timetabling review completed: Recommendations approved by October Ops Board and implementation being overseen by the DVC. Semester 2 starts action completed: Promotion process now in use ensures students on non-standard courses now have seamless access to moodle resources.	
19 (SW)	Negative assessment of curriculum compliance	Electronic document review completed: New actions around audit & set up.	
Goal 3: Employability: Ensuring students develop skills, aspiration and confidence.			
494 (SW)	Inconsistent delivery of Placement activity across institution	Impact reduced to medium	Schools On-boarding progress note: A dedicated Placement Officer joined the team in January and whose role is to focus on this activity, and to create and run the first user group this semester, as well as linking with the software User group for best practice.
Goal 4: Research & Enterprise: Delivering outstanding economic, social and cultural benefits from our intellectual capital.			
402 (PI)	2020 £ growth through Research & Enterprise	Student led audit of LDA completed. A number of actions now being implemented as a result. Entrepreneurial Comms action implemented: LSBU contracted external marketing agency to support awareness raising, & published an article in the THE regarding tenant engagement. AURA Action completed. 284 researchers completed AURA process, with 173 reporting ≥ 1 research output and 139 reporting ≥ 1 journal output. The data is now being used to inform University & School REF 2021 strategy.	Health CPD action progress note: The business case for a training company has been drafted, has been approved by the Executive, and is due for review at the next SBUEL board meeting.

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	<p>Internal Audit Actions implemented: All recommendations now incorporated into management processes.</p> <p>Ofsted insight action implemented: TQE appointment made to bring Ofsted insight within team, and LSBU not within current remit as no L2 & L3 programmes delivered to students < 19 years old, with student competency development offered through the UTC or local partner colleges.</p>	<p>Passmore Centre progress note: The Planning permission has been granted, contractors appointed, and agreements signed off, so progress on the refurbishment project is now underway.</p> <p>IPTE structure progress note: Pat Bailey appointed to national UCAS Advisory Group re apprenticeship application processes, which will help us inform marketing/recruitment strategies, and link to LSBU family approach.</p>
530 (DP)	Impact of LSBU family acquisition projects	Risk closed.	
Goal 6: Internationalisation: Developing a multicultural community of students & staff through alliances & partnerships.			
457 (PI)	International & EU student £income unrealised	New action around UKVI compliance	Financial model progress note: A draft model has been created, and this is being reviewed with a partner in Egypt for feedback in February prior to presentation to Executive.
517 (DP)	Impact of EU Referendum		
Goal 7: People & Organisation: Attracting proud, responsible staff, & valuing & rewarding their achievements.			
Page 185 2 (DP)	Response to environmental change & reputation	<p>Subject Pilot application action closed: LSBU was accepted as a participant by Hefce.</p> <p>Apprenticeships Action completed: Team now established 7 has overseen the launch of a range of Apprenticeship standards.</p> <p>Brand review action completed:</p>	
362 (ME)	Poor Staff Engagement	Likelihood reduced to low	
Goal 8: Resources & Infrastructure: Investing in first class facilities and outcome focused services, responsive to academic needs.			
2 (NL)	Home UG Recruitment income targets	<p>Brand Director appointed: Judith Barnard appointed as Director of Brand & Communications from 6th November.</p> <p>Brand Narrative developed, tested & presented to Executive: Now being further refined following market research feedback to increase appeal to target audience.</p> <p>New actions created for DARR.2 report, further narrative testing, and website re-fresh.</p>	<p>Market Insight research progress note: Meetings have been completed with all Schools, and Exec presentation scheduled on 1st February alongside related Estate plan.</p> <p>Corporate Comms plan progress note: Activity was postponed to ensure it could be led by the new Director of Brand and Communications, who is rethinking our approach to tendering for PR & will present to Exec in March. Team continues to increase positive coverage in the press.</p> <p>School & College Outreach progress note: New strategy in development following reviews of existing activity & gap analysis, due for completion by end Feb 2018, along with annual plan for managing MAT interactions by the end March.</p>

			<p>Brand Architecture progress note: Activity now led by DoB&C, who will present to Executive in March.</p> <p>Response protocols progress note: Activity now led by DoM&R, and will be completed by end February.</p> <p>Brand Campaign progress note: Recommendations developed through research groups, and initial briefing of HunterLodge agency carried out by interim Brand Consultant.</p>	
3 (RF)	Pensions deficit	<p>Actuarial advice action completed: Mercers have presented costed scenarios, which will be reviewed and presented to the next meeting of FP&R.</p> <p>Options review completed, and being presented to Executive meeting.</p>		
6 (RF)	Quality and availability of Management Information	<p>Student Record system action completed: A high level specification was developed to inform the Business case being reviewed by Exec in Nov.</p>		
Page 186	4 (WT)	Loss of NHS income	<p>Risk impact & likelihood reduced to medium</p> <p>New action around application processing</p>	<p>Health CPD action progress note: Re risk 402 - business case for a training company has been drafted, approved by Executive, & is due for review by SBUEL board meeting.</p>
	7 (RF)	Affordability of Capital Investment plans	<p>Funding options evaluated post recruitment:</p>	<p>Sinocampus action progress note: The steering panel is examining the merits of forming an educational joint venture to release capital to fund further studies, and will present an option to MPIC in March.</p> <p>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.</p>
305 (IM)	Corporate & personal data security & use	<p>GDPR Project manager appointed.</p> <p>Programme action added</p>		
584 (IM)	External incident compromises campus operations or access	<p>Controls updated:</p>		

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	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: Sustained underinvestment in expertise and dedicated human resource to support utilisation of learning technologies, comparative to new and existing competitors.</p> <p>Effect: 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 deliver new provision such as apprenticeships Curriculum do not adapt sufficiently to remain relevant, jeopardising the employability of LSBU graduates. More flexible and efficient educational models which enable us to remain adaptable and competitive are out of institutional reach 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. Market appeal of courses is impaired, impacting negatively on recruitment.</p>	I = 2 L = 2 Medium (4)	<p>CRIT (Centre for Research Informed Teaching) reports regularly to the Student Experience Committee & to the Quality & Standards Committee on the Achievements of work undertaken.</p> <hr/> <p>Delivery of the Technologically Enhanced Learning Strategy (TEL) through the Educational Framework and Quality Processes, monitored by Academic Board.</p>	I = 2 L = 2 Medium (4)	Increase organisational capability for utilising lecture capture technology, through champions in all divisions trained in appropriate technology.	Saranne Weller	31 Jul 2018
							Complete activity to establish a baseline across all modules for core digital enhanced learning practice.	Saranne Weller	31 Jul 2018
							Deliver professional development for course directors.	Saranne Weller	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
467	Progression rate across undergraduate programmes does not rise in line with targets of Corporate Strategy	Shan Wareing	<p>Cause: Students admitted through clearing with lower tariff and less commitment to the course. High risk students are not identified in a timely way and supported sufficiently. Failures in timetabling, organisation and communication increase during periods of change, and high risk students are more vulnerable. New initiatives don't engage students. Provision fails to meet immediate needs of students entering through non-traditional access routes. Unable to finance student support adequately to meet level of demand.</p> <p>Effect: Progression rate fails to increase sufficiently . HEFCE, or OFS could view LSBU as high risk. Data could have negative impact in TEF metric assessment. Considerable loss of income from UG non-progression to level 5 and 6.</p>	I = 3 L = 2 High (6)	Student Welfare advice and support provided by Student Life Centre	I = 3 L = 2 High (6)	Review current Job Description for Course Directors, ensuring fit with current priorities and Career Pathway structure.	Shan Wareing	22 Dec 2017
					Study Support & Skills Sessions provided by the Library & LRC		Oversee amendments to progression information stored in data warehouse, conduct testing, and export for presentation within Board Report.	Richard Duke	28 Feb 2018
							Oversee development of revised MIKE dashboards with new progression dimensions, and embed within core planning cycles and present to Quality & Standards committee.	Richard Duke	31 May 2018
							Implement a minimum specification for personal tutoring, ensuring consistent student support & increasing progression rates.	Shan Wareing	31 Jul 2018
							CRIT to work with Schools and course teams to embed learning development in targeted courses or high impact modules with pass rates less than 40%.	Saranne Weller	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
518	Core student systems have limited flexibility for market adaptation or rely on manual work arounds	Shan Wareing	<p>Cause: Core course administration processes & systems (QL, timetabling, Moodle, MyLSBU) require manual and emergency interventions to function. Non standard delivery challenges existing protocols and procedure. System infrastructure limitations, or slow change mechanisms may not meet all the needs of emerging delivery models, from student or management perspective</p> <p>Effect: Lack of clear information provision to students and staff, with negative impact on student experience & reputational damage. Students fail to attend teaching sessions, submit work on time or receive marks, so progression suffers. Staff compensating for systems failures, or inventing work arounds are distracted from other activity leading to failures elsewhere. Staff morale suffers and sickness rate and turnover rate increase.</p>	I = 2 L = 3 Medium (6)	Operational Issues reported and tracked through ICT TopDesk system, with internal escalation protocols. SRS Replacement Project Updates scrutinised at Academic Board, to oversee progress and assess fit with strategy and existing practice.	I = 2 L = 2 Medium (4)	Review possibility of utilising the automated functions of CMIS timetabling system. Implement a modern student enquiry management approach, to deliver a holistic approach to information provision and query management	Simon Francis Kirsteen Coupar	31 Jan 2018 31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
519	Negative Assessment of Curriculum Compliance	Shan Wareing	<p>Cause: Transition to OfS regime could result in new approach to monitoring or review, or to standards. Increase in activity could lead to overstretched teams and a failure to complete adequate quality processes in the Schools or PSGs. Academic staff insufficiently prepared for quality processes, (new to HE or lack of appropriate professional development). Significant changes to curriculum not processed through formal mechanisms. High risk activity with partners (placement, international partners, UK partners (particularly FE or schools education) does not have adequate resource or expertise allocated to it to identify and manage risks.</p> <p>Effect: Quality code processes not followed, leading to failures in quality, and negative external assessment. Negative impact on Board of Governors ability to sign off OfS assurances or returns. Potential for unwelcome result from Annual Provider Review, TEF process submissions, or indeed achievement of OfS registration conditions, impacting on University status. Leading to negative impact on income & reputation, through recruitment levels, and differing fees. Negative judgement by Competition and Markets Authority and cost of legal challenge. Could act as barrier to recruitment of international students, further affecting income and reputation.</p>	I = 3 L = 3 High (9)	Academic Audit process monitored by Academic Board via periodic reports from Quality & Standards Committee (QSC).	I = 3 L = 1 Medium (3)	<p>Conduct full audit of Course Specification documents against Live Course list from QL.</p> <p>Oversee transition of Curriculum Set up responsibility into the Registry team.</p> <p>Oversee translation of all existing course specifications into new Educational Framework format, incorporating CRIT guidance principles, to ensure parity with newly validated courses.</p>	Sally Skillett-Moore Ralph Sanders Janet Bohrer	22 Dec 2017 31 Jul 2018 31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
494	Inconsistent delivery of Placement activity across institution	Shan Wareing	<p>Cause: Insufficient human resource allocation centrally and in Schools Insufficient expertise within LSBU. Lack of allocation of sufficient central and School human resource. Speed of implementation without underpinning project planning or learning from the sector. Lack of assurance over offsite workplace conditions.</p> <p>Effect: Placement practice may not comply with Chapter B10 of the Quality Code, so may be a quality risk. LSBU may not be able to provide a placement, internship or professional opportunity for all UG students entering in 2016 and after, leading to a CMA risk Placements may not deliver a good student experience, creating a risk to achievement of NSS improvement plans. Duty of care to students re workplace safety may not be met, creating a reputational risk. Potential insurance risk.</p>	I = 2 L = 2 Medium (4)	Utilisation of new software platform 'InPlace' enables efficiencies in the Schools & the centre, and supports constancy of process and knowledge sharing.	I = 2 L = 1 Low (2)	Complete onboarding of remaining Schools to InPlace Operational procedures and User Group.	Sukaina Jeraj	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	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. <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. 	I = 2 L = 2 Medium (4)	<p>Bid writing workshops for academic staff delivered routinely</p> <hr/> <p>Enterprise Business Plan & strategy submitted for approval annually to Operations Board.</p> <hr/> <p>Operation of Sharepoint Enterprise Approval Process for authorisation of new income opportunities.</p> <hr/> <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>	I = 2 L = 2 Medium (4)	<p>Establish a CPD offering for Health Professionals in collaboration with School of Health & Social Care.</p> <hr/> <p>Oversee submission of bids for LURN partnerships.</p> <hr/> <p>Establish revised operating structure for new SBUEL+ enterprise subsidiary.</p> <hr/> <p>Oversee appointment of LDA student representatives for each School.</p> <hr/> <p>Oversee recruitment of Director for Health Innovation Lab, a new SBUEL entity, to establish a more professional and sustainable approach to HSC CPD provision.</p> <hr/> <p>Oversee submission for aceeu.org accreditation. (Accreditation Council for Engaged & Entrepreneurial Universities)</p>	Paul Ivey	30 Nov 2017
								Graeme Maidment	22 Dec 2017
								Paul Ivey	31 Jan 2018
								Graeme Maidment	30 Mar 2018
								Paul Ivey	30 Apr 2018
								Gurpreet Jagpal	31 Aug 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
495	Impact of Higher Apprenticeship degrees on existing recruitment markets	Pat Bailey	<p>Cause: The Introduction of Higher Apprenticeship degrees may present an opportunity for LSBU to grow student numbers in a new market. Offering and administrating apprentice schemes requires compliance with SFA funding regulations, with revised funding models depending on successful EPAs, and opens up new areas of the institution to scrutiny from Ofsted.</p> <p>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. SFA audit failure could lead to funding clawback, and Ofsted inspection failure could lead to reputational damage.</p>	I = 3 L = 1 Medium (3)	6 monthly progress report from Apprenticeships Steering Group scrutinised by Academic Board covers IPTE and Passmore Centre.	I = 3 L = 1 Medium (3)	Determine structure of IPTE when shape of LSBU family confirmed.	Pat Bailey	30 Sep 2018
					Monthly meetings of Apprenticeships Committee review all related operational matters.		Arrange launch of Passmore Centre following refurbishment programme.		

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
457	Anticipated international & EU 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. TNE partnerships are not approved, present quality risks, or break down due to absence of adequate support structures, or when contacts relocate.</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. TNE enterprise expectations unrealised.</p>	I = 3 L = 3 High (9)	<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 <hr/> <p>International & EU recruitment Reports presented to each meeting of Ops Board.</p> <hr/> <p>International Office runs annual cycle of training events with staff to ensure knowledge of & compliance with UKVI processes.</p> <hr/> <p>Regular reporting of Visa refusal rates to Director of Internationalisation by Immigration Team.</p>	I = 3 L = 3 High (9)	Ensure financial model for partnerships recognises the costs of managing risks to quality and the student experience.	Paul Ivey	01 Aug 2017
							Engage external consultant to advise on overarching compliance approach with single point of contact for both Tier 2 & Tier 4 activities.	Paul Ivey	28 Feb 2018
							Develop new institutional partnerships with EU partners.	Stuart Bannerman	31 May 2018
							Establish up to 5 overseas offices, with common management oversight and reporting lines.	Stuart Bannerman	31 Jul 2018
							Oversee Internationalisation campaign across LSBU Schools.	Stuart Bannerman	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	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.</p> <p>Effect: 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. 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. 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 and limit access to structural funds. Legislative Compliance: There could be additional administration cost in updating many EU compliant processes if regulations are amended. Impact on bond yields could affect year end pension liabilities.</p>	I = 2 L = 3 Medium (6)	Use of London economic models to estimate impact on student recruitment and model reductions in EU student numbers and identify mechanisms to compensate	I = 2 L = 1 Low (2)	Develop strategic plan for marketing and support of EU student cohort, preparing for future removal of student loan funding mechanism.	Stuart Bannerman	30 Mar 2018
							Add 4 academic leads to Research Institutes, to build strategic relationships with UKRI, UK research Councils and UK (Russell Group) HEIs.	Gurpreet Jagpal	30 Apr 2018
							Monitor situation with regard to employment law and right to work, and ensure that appointments are made in compliance with any changes to regulation.	Mandy Eddolls	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
1	Organisational responsiveness to policy changes, external perception & shifts in competitive landscape	David Phoenix	<p>Cause:</p> <ul style="list-style-type: none"> - Changes to fees and loan funding models - Transition to OfS as sector regulator and risk based assessment approach - Increased competition from Private Providers and other HEIs post SNC - The Apprenticeship Levy & programme development - Evolving external assessment through TEF mechanisms - Failure to anticipate change - Failure to position (politically) & (capacity/structure) <p>Effect:</p> <ul style="list-style-type: none"> - Reduced student recruitment - Failure to differentiate provision - Workforce out of alignment with portfolio - Impaired external recognition through subject level tef - Burden of response to regulatory intervention, and potential impact or outcome of decision - Registration failure with OfS leading to loss of University Title and access to current levels of funding. 	I = 2 L = 3 Medium (6)	<p>Annual articulation of corporate strategy by Executive through Corporate Roadmaps.</p> <hr/> <p>Chief Marketing Officer on Executive leads strategic development of brand and portfolio.</p> <hr/> <p>Corporate Affairs unit maintain relationships with key politicians and influencers, in local boroughs and amongst FE providers.</p> <hr/> <p>Financial controls, forecasting process & restructure capacity enable tracking of forward operating surplus target.</p> <hr/> <p>Horizon scanning report produced weekly by the Corporate Affairs Unit</p> <hr/> <p>Local Roadmap alignment with Corporate Roadmaps ensures linked strategic focus across operational areas, with 6 monthly Organisation Effectiveness reviews by VC.</p> <hr/> <p>PPA team provide Senior Managers with trend analysis & benchmarking against KPIs, and access to MIKE platform for information analysis.</p>	I = 2 L = 1 Low (2)	<p>Oversee introduction of new portfolio relating to new division of Creative Industries, including fashion promotion.</p> <hr/> <p>Engage with Subject level TEF panels to inform LSBU approach (with Shan Wareing).</p>	Janet Jones	30 Apr 2018
								Pat Bailey	30 Apr 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
362	Low staff engagement impacts performance negatively	Mandy Eddolls	<p>Cause:</p> <ul style="list-style-type: none"> •Systems and structure do not facilitate teamwork between areas of the University •Staff feeling that they do not have easy access to relevant information directly linked to them and their jobs •Poor pay and reward packages •Poor diversity and inclusion practises •Limited visibility of Leadership •Lack of quality physical estate <p>Effect:</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)	<p>Internal Comms campaign to promote Employee engagement using #wevalueyourvoice.</p> <hr/> <p>Cascade messages from Ops Board circulated for Cascade / Congress / Town Hall Meetings within each School & PSG.</p> <hr/> <p>Direct staff feedback is encouraged through the Continuing the Conversation VC events, & through discussions on Yammer.</p> <hr/> <p>Employee engagement champions established for each Shools & PSG with regular network meetings to actively support engagement initiatives.</p> <hr/> <p>New social spaces and forums for staff established.</p> <hr/> <p>Planning process promotes golden thread connection from Corporate Strategy, through Roadmaps to Staff Appraisal.</p> <hr/> <p>RAG progress reports from 3 themed institutional plans, and School & PSG action plans, are monitored at every other Operations Board meeting.</p>	I = 3 L = 1 Medium (3)	Oversee procurement of 3rd party web portal to deliver benefit packages to staff.	Mandy Eddolls	28 Feb 2018

Standard Risk Register



Page 198

Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
2	Course portfolio, or related marketing activity and admissions processes do not achieve Home UG & PG recruitment targets	Nicole Louis	Cause: <ul style="list-style-type: none"> - Increased competition from selective institutions and private providers - Failure to articulate compelling brand to applicants - Long term payback period of re-positioning activity - Declining applicant pool - Excessive churn within MAC workforce - Lack of ability to anticipate demand and re-shape provision. - Negative reputational impact of unmanaged external events - Portfolio or modes of delivery not aligned with market demand - Change to historic conversion levels amongst applicants - Limited internal focus on PG developments & recruitment - Impact of differentiated fees on applicant behaviour Effect: <ul style="list-style-type: none"> - Under recruitment against targets - Related loss of income, and impact on corporate ambitions - Undermining of course profitability 	I = 4 L = 3 Critical (12)	Advance predictions of student recruitment numbers informs the Annual five year forecast submitted to Hefce each July	I = 4 L = 3 Critical (12)	Present outputs of Market Insight Research Project to School Management teams and take recommendations to Executive Workshop.	Nicole Louis	31 Oct 2017
					Annual QSC approval of validation cycle informed by market insight		Plan for corporate comms shared with Executive.	Judith Barnard	30 Nov 2017
					Conversion trend data analysis allows identification of target areas for focus and resource.		Develop revised School & College Outreach Strategy, with broader footprint outside local boroughs, which includes LSBU Family MAT institutions.	Sarah Gordon	30 Nov 2017
					Cycle of School student number reviews, allow MAC stress testing of TM1 enrolment forecasts, and development of joint targets for next recruitment cycle.		Re-engineer response protocols for all applicants, with revised process statement and related messaging.	Steven Brabenec	31 Jan 2018
					DARR applications report presented to Operations Board & reviewed by FP&R Committee.		Executive review of proposal for LSBU Brand Architecture.	Judith Barnard	31 Jan 2018
					Fortnightly Marketing Operations Board reviews latest applications cycle data.		Oversee testing and launch of DARR phase 2 report, to provide re-formatted user friendly presentation of recruitment cycle data (application & enrolment) at Institution, School and Course level.	Alex Steeden	28 Feb 2018
					Weekly recruitment summary circulated to Executive.		Oversee completion of 'Look & Feel' refresh of printed prospectus, and external website, to incorporate update of key navigation.	Steven Brabenec	28 Feb 2018
							Complete revision of School web page content & imagery.	Steven Brabenec	30 Mar 2018
							Oversee further refinement of Brand Narrative, conduct testing, and present results to Executive.	Judith Barnard	30 Apr 2018
							Develop creative institutional brand campaign with revised narrative and brand architecture for start of next cycle.	Nicole Louis	31 Jul 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
3	Staff pension scheme deficit increases	Richard Flatman	<p>Cause:</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 - Further change to accounting requirements for TPS & USS schemes <p>Effect:</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>Annual FRS 102 valuation of pension scheme</p> <hr/> <p>DC pension scheme for SBUEL staff.</p> <hr/> <p>Regular monitoring of national/sector pension developments and attendance at relevant conferences and briefing seminars by FMI Management team.</p> <hr/> <p>Regular participation in sector review activity through attendance at LPFA HE forum, BUFDG events & UCEA pensions group by CFO or deputy.</p> <hr/> <p>Reporting to every Board of Governors meeting via CFO Report</p> <hr/> <p>Strict control on early access to pension at redundancy/restructure</p> <hr/> <p>Tight Executive control of all staff costs through monthly scrutiny of management accounts</p>	I = 3 L = 2 High (6)	<p>Presented Mercers costed scenarios to the next meeting of FP&R.</p> <hr/> <p>Present HR options review paper to Executive.</p>	Richard Flatman	27 Feb 2018
								Mandy Eddolls	28 Feb 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
6	Management Information is not meaningful, reliable, or does not triangulate for internal decision or external reporting	Richard Flatman	Cause: - Lack of understanding of system dependencies - 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 Effect: - 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 every 6 months to review matters of data quality and provides reports to Operations Board.	I = 3 L = 1 Medium (3) 	Develop and circulate a set of performance scorecards for Professional Service Groups and Schools, for review at Operational Effectiveness Meetings.	Richard Duke	31 May 2018
					Internal Auditors Continuous Audit programme provides regular assurance on student and finance information, including UKVI compliance.		Deliver phase 2 of MIKE data programme, to incorporate Financial and HR data in management platform, with related dashboards for management teams.	Richard Duke	29 Jun 2018
					Sporadic internal audit reports on key systems through 3 year IA cycle to systematically check data and related processes: - HR systems - Space management systems - TRAC - External returns <hr/> Systematic data quality checks and review of external data returns prior to submission to HESA by PPA team.		Established revised corporate dataset and related dashboard within MIKE for monitoring applications & associated income flows for 2019/20 entrants.	Richard Duke	21 Dec 2018





Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
14	Loss of NHS contract income	Warren Turner	<p>Cause: NHS financial challenges/ structural changes resulting in a total review of educational commissioning by Health Education England with an expected overall reduction in available funding (affecting CPPD). London Educational Contract bursaries ceasing for new Pre-Registration students from Sept 2017, with students accessing student loans. Loss of placement capacity.</p> <p>Effect: Recruitment to contracted programmes could dip following shift away from bursaries to tuition fees, leading to reduction in income. Reduced quality of applicants Reduced staff numbers Reduced student numbers</p>	I = 2 L = 3 Medium (6)	<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> <hr/> <p>Monitor quality of courses (QCPM and NMC) annually in autumn (QCPM) and winter (NMC)</p> <hr/> <p>Named Customer Manager roles with NHS Trusts, CCGs and HEE, managing relationships including placement provision.</p> <hr/> <p>Support provided to applicants with numeracy and literacy test preparation.</p>	I = 2 L = 2 Medium (4)	<p>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</p> <hr/> <p>Lead project with Guy's & St Thomas's Hospitals NHS Foundation Trust to develop a 16-18 Cadetship Apprenticeship which will also provide links to FE providers locally, and to health careers/ courses at LSBU.</p> <hr/> <p>Oversee enhanced approach to processing NHS contract applications, with improved response times for testing and offer making.</p> <hr/> <p>Havering lease - EAF dealing with negotiations with NHS Properties - extension of lease to 2023 had been offered. Potential for further/ alternative location at either Care City site (Barking) or Purfleet New Town site.</p>	Warren Turner	25 Sep 2017
								Lesley Marsh	31 Oct 2017
								Kathryn Gilmore	31 Aug 2018
								Warren Turner	27 Sep 2021

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
37	Affordability of Capital Expenditure investment plans	Richard Flatman	Cause: - Poor project controls - Lack of capacity to manage/deliver projects - Reduction in agreed/assumed capital funding - Reduction in other government funding Effect: - Adverse financial impact - Reputational damage - Reduced surplus - Planned improvement to student experience not delivered - Inability to attract new students	I = 3 L = 3 High (9) 	Capex reporting is embedded into management accounts provided to each meeting of the FP&R Committee, & into financial forecasts approved annually by Board. Estates & Academic Environment PSG have local project methodology, with project controls, & governance applied to all Capex projects. Financial regulations require all major (>£2m) capital expenditure to receive Board approval Full Business Cases prepared; using Executive approved process - including clarity on cost and funding, for each element of Estates Strategy. Major Projects & Investments Committee (MPIC) reviews all property related capital decisions, and is empowered to approve all unplanned capital expenditure > £500K but <£1M.	I = 3 L = 1 Medium (3) 	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.	Ian Mehrtens	30 Apr 2013
							Test Sinocampus options for Technopark building.	Paul Ivey	30 Nov 2017
							Work with Finalysis to develop loan funding proposals.	Richard Flatman	31 Jan 2018
							Test market opportunity for disposal of Perry Library site.	Ian Mehrtens	31 Jan 2018
305	Corporate & personal data not accessed or stored securely, or processed appropriately	Ian Mehrtens	Cause: Unauthorised access to data Inappropriate use of personal data Loss of unencrypted data assets Breach of digital security; either en masse (e.g. cyber attacks) or specific cases (e.g. phishing scams) Regulatory failure Use of unsupported storage locations Effect:	I = 3 L = 2 High (6) 	A privacy impact assessment is a required stage of the ICT project initiation process. All changes to digital infrastructure reviewed quarterly by ICT Technical Roadmap Board.	I = 3 L = 1 Medium (3) 	Oversee complete upgrade of all remaining Windows XP and Windows 2003 machines.	Craig Girvan	22 Dec 2017
							Oversee presentation of GDPR project programme to Executive team.	Olajide Iyaniwura	31 Jan 2018
							Oversee recruitment of new Data Protection Officer	James Stevenson	30 Mar 2018

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
			<p>Financial penalty under General Data Protection Regulations.</p> <p>Cost and impact of staff resource diverted to deal with issues, Staff downtime when systems unavailable</p> <p>Reputational damage, undermining academic credibility.</p> <p>Compromise of competitive advantage.</p>		<p>IT access permissions linked directly with live iTrent HR system records through Active Directory account synchronisation.</p> <hr/> <p>Logical security protocols relating to passwords require change every 6 months, and multiple character combinations.</p> <hr/> <p>Quarterly Mandatory Training Compliance reports are circulated to all Level 2 managers, which includes information on staff compliance with training on data protection and data security.</p> <hr/> <p>Robust breach notification process to close down & contain any breach.</p> <hr/> <p>Weekly Change Control Board chaired by Director of ICT Services reviews all proposed technical changes to infrastructure prior to implementation.</p> <hr/> <p>Weekly running of infrastructure vulnerability management software test results reviewed by Head of Digital Security</p>				

Standard Risk Register



Risk Ref	Risk Title	Risk Owner	Cause & Effect	Inherent Risk Priority	Risk Control	Residual Risk Priority	Action Required	Person Responsible	To be implemented by
584	External incident compromises campus operations or access	Mandy Eddolls	<p>Cause: Incident in South London area requires emergency response and restricts freedom of movement</p> <p>Effect: Staff & students unable to reach / leave the campus Interruption to key activities or processes Requirements for alternative accommodation / provision for halls residents</p>	I = 2 L = 2 Medium (4)	<p>Building Lockdown plans in place for implementation by the Security Team as required.</p> <hr/> <p>Business continuity plans for critical activity reviewed annually by resilience team.</p> <hr/> <p>Emergency Information sets present at every reception building on campus (Floor Plans, Loudhailers & Hi-Vis Jackets)</p> <hr/> <p>Halls Accommodation aid agreement in place with London School of Economics.</p> <hr/> <p>Major incident response mechanisms – tested annually.</p>	I = 2 L = 2 Medium (4)	Conduct Emergency Planning Scenario Exercise with Executive Team.	Edward Spacey	28 Feb 2018

	CONFIDENTIAL
Paper title:	External audit progress report
Board/Committee:	Audit Committee
Date of meeting:	8 February 2018
Author:	KPMG
Sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	To note
Recommendation:	The Committee is requested to note the report.

Executive Summary

The committee is requested to note the progress report.

This page is intentionally left blank



Progress Report and Technical Update

London South Bank University
External Audit 2017-18
February 2018

External Audit Progress Report – February 2018

Since the last Audit Committee on 9 November we have...

- Concluded our 2016/17 audit, and signed our opinions on the University and SBUEL accounts;
- Prepared our risk management benchmarking exercise, which will be presented to the next meeting of the Audit Committee; and
- Arranged to meet with management to debrief the 2016/17 audit and plan our 2017/18 audit.

Ahead of the next meeting of the Audit Committee in June 2018 we will have...

- Met with management to agree the timing of our interim and final audit visits; and
- Completed our planning procedures and prepared our Audit Plan for 2017/18.

Actions arising from this report

We ask the Audit Committee to:

- **NOTE** this progress report; and

Contacts

Fleur Nieboer

Partner

07768 485532

Fleur.Nieboer@kpmg.co.uk

Jack Stapleton

Manager

07468 750121

Jack.Stapleton@kpmg.co.uk

Issue	Impact and insight
<p><i>Universities: Harnessing their superpowers</i></p> <p>Universities are an undervalued force for development. With a presence in nearly every major town and city in the world, they should be at the centre of regional regeneration and international partnership building. But too often the potential powers they have are overlooked.</p> <p>Although some universities are leading the way in city-building efforts, more needs to be done to deliver the full benefit for both universities and the places in which they operate.</p> <p>Looking to Toronto as a global example, this report gives some concrete examples of how universities' hidden superpowers can be deployed:</p> <ul style="list-style-type: none"> • How universities can team up with cities to solve societal challenges – and why it's so urgent that they do; • What can be achieved when all the universities in a city come together, for example on a single research project; • How some universities are blurring the lines between campus and city: anything from a laboratory for the city to cinematic lecture theatres; • How universities can be a 'window on the world' for the place in which they operate - and how partnerships that cross the globe benefit relations with partners on the university's doorstep; and • The forces that are shaping future local decision making: from city diplomats to powerful city ministries and how universities can engage with them. <p>Download the full report at https://home.kpmg.com/uk/en/home/insights/2017/11/universities-harnessing-their-superpowers.html</p>	<p>This is the latest piece of thought leadership on the higher education sector from KPMG.</p> <p>There are no specific actions for LSBU to take, but the report may be of interest to the University.</p>



© 2018 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Paper title:	South Bank Academies Audit Report
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Natalie Ferer, Financial Controller
Executive/Operations sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	To report on the audit of the South Bank Academies accounts and to present the audit report prepared by the Trust's auditors, Kingston Smith.
Recommendation:	The committee is requested to note the report.

Summary

For information, the audit report for South Bank Academies is attached. While Kingston Smith, the external auditors, have issued an unqualified audit opinion, they encountered significant difficulties during the course of the audit. 18 audit recommendations have been made, 9 of which are rated as high risk and a plan is underway to implement these recommendations

Background

South Bank Academies (SBA) is part of the LSBU family of institutions but is a separate legal entity and its financial results are not consolidated with the University's. However, LSBU and its staff are represented on the SBA Board, Audit Committee and on the Local Governing Bodies of the two schools within SBA and therefore some oversight is required given the reputational risks involved.

Following the resignation of the previous SBA Business Manager, a replacement was recruited and started employment in June 2017. A smooth transition was not possible. This, and a combination of other factors, contributed to a breakdown in controls with significant gaps on the oversight of control, financial operations, and data quality.

The initial deadline for filing accounts with the ESFA was not met, although these have now been signed and submitted.

Action to address control weaknesses

Most of the recommendations relate to improving financial procedures and strengthening financial control. Implementation is being monitored closely by the University Financial Controller and the attached management letter forms the basis of the action plan to prevent reoccurrence.

Financial control is a local responsibility but it is clear that control processes need to be strengthened and, where possible, brought into line with those in place within the University. There is an ongoing discussion around 'Groupness' and the LSBU family of institutions and the recommendation is likely to be that we move to a group wide professional services function with a SBA Finance business partner and close oversight by the University Financial Controller.

In the meantime, the University's Financial Control team are now overseeing financial control and reporting processes within SBA in order that the accounts are brought up to date and so accurate management accounts can be produced for management and directors. It is also planned that the University team will manage the year end and audit process and oversee production of the 2017/18 SBA accounts.

A report on progress will go to the next SBA Audit Committee on 6 March 2018.

Recommendation

The Committee is requested to note this report.

South Bank Academies

Post Audit Management Report

Year Ended 31 August 2017

Post Audit Management Report – South Bank Academies

We have completed the audit of South Bank Academies (SBA) for the year ended 31 August 2017 and whilst we expect to issue an unqualified audit opinion on our Kingston Smith Audit report, there have been significant difficulties encountered which have been identified throughout his report.

As part of our audit work and in accordance with the reporting requirements outlined in the regularity report we have identified irregularities in relation to the maintenance of the books and records and the management information being reported to the Board. We have highlighted key areas of concern in Section 2 and Section 3 of this report, with further details outlined in the appendices. An explanation of the issues has been included in the Financial Statements by the Directors.

We understand that the Trust is in the process of bringing their accounting system up to date and a more rigorous internal control process is to be introduced once this exercise has been completed.

This report covers the findings from our audit, the scope of which was communicated to you prior to commencing the work. It includes a number of points which have been deemed to be high and medium risk which need to be resolved.

If you have any concerns or questions arising from this report, please contact Anjali Kothari.

Yours faithfully

.....
Kingston Smith LLP

.....
Date

Contents

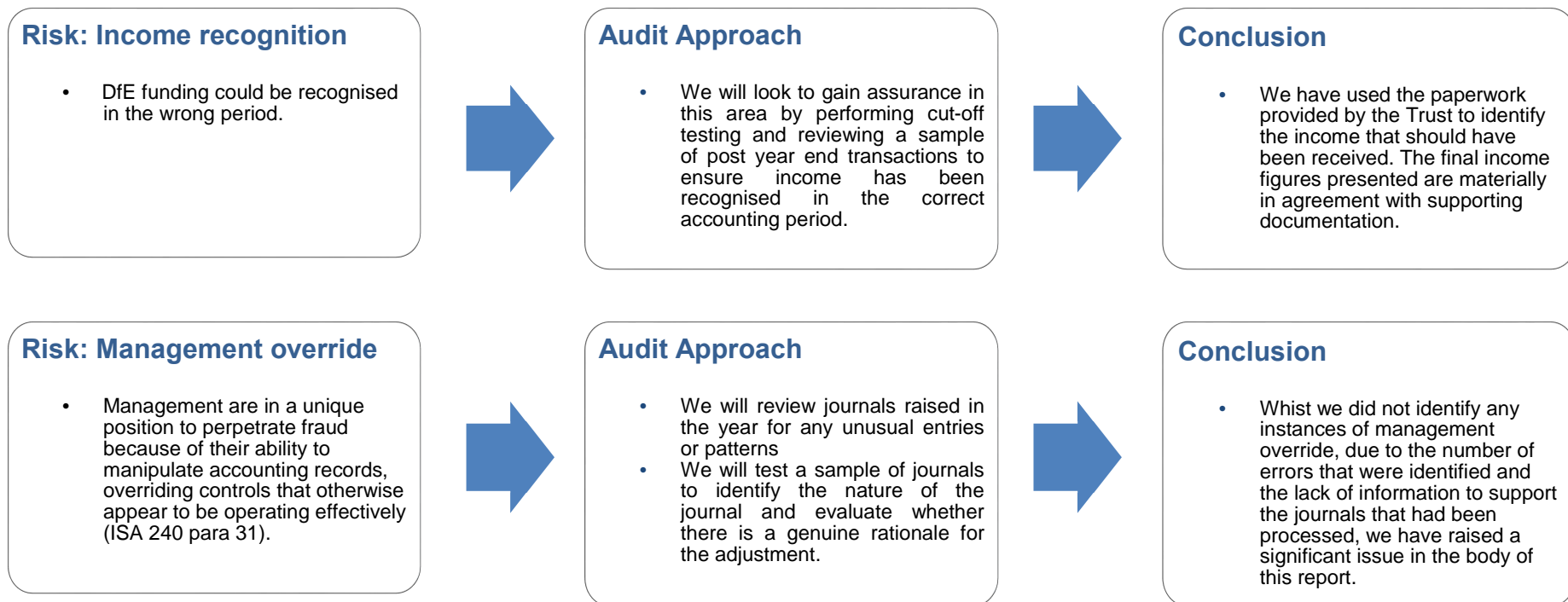
Section 1	Audit Approach
Section 2	Significant findings from the Audit
Section 3	Operation of the Accounting and Internal Control Systems
Section 4	Operation of the Accounting and Internal Control Systems – follow up on prior year points raised
Section 5	Sector update
Appendix 1	Corrected Misstatements and Reclassifications from the ETB
Appendix 2	Uncorrected Misstatements and Reclassifications
Appendix 3	Other matters

Section 1: Audit Approach

As outlined in our pre-audit letter dated 9 June 2017 our audit approach is based on an assessment of the audit risk relevant to the individual financial statement areas. Areas of risk are categorised according to their susceptibility to material misstatement, whether through complexity of transactions or accounting treatment. For each area we calculated a level of testing and review sufficient to give comfort that the financial statements are free from material misstatement.

The following table lists any risks identified at the planning stage and during the course of the audit, our approach to mitigate the risk and our conclusions from completing this work. Unfortunately due to the difficulties encountered as part of the audit process as identified in section 2 and 3 of this report, and from the work that we have undertaken ourselves we believe that the conclusions we have reached have to be referenced to the detail issues raised within this report.

Page 216



Section 2: Significant Findings From The Audit

We are required under International Standards on Auditing to request you to correct all misstatements identified during our audit, with the exception of those that are clearly trivial.

Corrected material misstatements and reclassifications

As referred to in the Significant difficulties section, the original trial balance presented for audit was not reflective of the year's results

Management were not able to correct the system on a transactional level within the time frame, but prepared reconciliations and breakdowns for balance sheet items and identifiable areas such as income and payroll. A manual extended trial balance was created to record all the adjustments identified from the work undertaken, in order to bring the figures to the correct year end position.

This revised trial balance was then audited, and included as Appendix 1 are the corrected misstatements identified during the course of our audit work which have been discussed and agreed with you.

Uncorrected immaterial misstatements and reclassifications

Included as Appendix 2 are the uncorrected, immaterial misstatements and reclassifications identified during the course of our audit work.

Observations concerning the operation of the accounting and control systems

We detail in section 3 other matters concerning the operation of the accounting and control systems that we consider should be brought to your attention. The observations have been ranked in order of potential risk to the Trust.

We look forward to receiving your responses on the points raised.

Due to the nature of an audit we may not have identified all weaknesses within the accounting and internal control systems which may exist and the contents of this section of our letter and any items disclosed in this report should not therefore be taken as a comprehensive list of such weaknesses.

Significant difficulties

We experienced significant difficulties and delays during our audit as the financial information presented to us was incomplete and could not be supported by the underlying financial records.

The original trial balance presented for audit was not reflective of the year's results and a number of the key control accounts had not been reconciled or reviewed and a significant number of postings were errors, duplicate transactions or incomplete.

The answers given to some of the audit queries and requests made have been inadequate and indicate a lack of understanding of the underlying issues, or are reflective of the lack of a full audit trail throughout the year.

Under significant matters we have summarised the key issues. Under section 3 we have provided more detail on the individual issues we faced.

Section 2: Significant Findings From The Audit

Significant matters

The number of significant issues noted within this report as well as the state of the financial records indicate that no adequate internal reviews had been undertaken by an independent person during the year, which would have identified the issues sooner. It also indicates the lack of systematic controls and processes that should be undertaken on a weekly/monthly basis. For example the payroll journals had not been fully posted onto the accounting system since April 2017. However if the net wages control account was being reconciled as part of the normal controls process, this issue would have been identified by May 2017 at the latest.

Another example includes the purchase ledger control account which included a number of duplicate entries, payment only entries and outstanding invoice payments where invoices had been paid directly through the bank. A review of the ledger and a process to reconcile it to the trial balance would have identified the discrepancies at a much earlier stage.

As part of the issue the bank accounts had not been properly reconciled within the accounting system and therefore a number of incorrect transactions had not been identified on a timely basis. In addition a bank account previously in use under the UTC was still active but had not been included in the financial statements as it was not thought to have been dormant during the year.

As part of our audit work and in an attempt to unravel some of the errors identified it became apparent that there was a lack of clarity and information, and therefore an appropriate audit trail for journal entries, including income and opening balances.

With the number of errors identified it became clear that the Directors could not have received accurate financial information which correlated to the accounting system during the year, therefore the management accounts must have been incorrect during and post year end.

The extent of the issue was quite significant. Whilst a number of errors have been identified and corrected, there are still areas of the accounts that whilst materially correct based on the information we have to date, we cannot be certain will not result in a prior year adjustment in the following year. For example we are unable to ascertain whether an accrual of £111k is an accurate charge for the light and heat used and if so which nominal code the remainder of the accrual has been posted to as the current nominal expense code only reflects £58k of costs for this year.

Future risks

The Trust has taken the decision from October 2017, when the extent of the issue became apparent, to maintain the financial records on a manual ledger via excel rather than continue to maintain its current accounting system, PS Financials. We understand that part of this decision is because the accounting package has to be updated to a more current version.

Given the size of the Trust maintaining a manual accounting system is high risk as it is prone to human error. It is more difficult to maintain and produce the financial information on an accruals and prepayments basis and is not a robust system for cash management against budgets, and projections.

Section 2: Significant Findings From The Audit

We would strongly advise that the Trust reverts back to using its current accounting system, update the accounting entries from October 2017 and run the proper checks, reconciliations and processes to ensure all the information is correct and accurate with a proper audit trail.

Management Representation Letter

A draft of our proposed management representation letter has been sent to you under separate cover. All of the matters included in this letter on which we seek the Trustee's formal confirmation are in respect of routine matters, except for the following:-

Point 7 – we only refer to material transactions as opposed to all transactions

Point 8 has been expanded to refer to donated services and South Bank University

Point 9 has been included to capture the transactions with South Bank University

Point 11 – we have sought further confirmation that we have all the information we need in respect to the notional rent for South Bank Engineering UTC

Point 14 – We have asked you to confirm that you do not anticipate any material adjustments to the pension report from Hymans Robertson LLP for their early recognition of your pension contribution of £22k

Point 15 – We have asked for you to confirm the accrual of £111k for light and heat is valid based on the information available to you at the time of signing this letter.

Point 17 - We have asked you to confirm that the actuarial assumptions used by the actuaries Aon Hewitt Limited and Hymans Robertson LLP in calculating the actuarial movements, and fair values of the assets and liabilities of the local government defined benefit pension schemes are consistent with our knowledge of the trust.

Point 28 – The point has been expanded to take note of the additional wording relating to the Regularity audit report in the financial statements

Point 29 – the point has been expanded to include reference to materiality.

USEFUL OBSERVATIONS

Members

We would note that the ESFA recommends a minimum of 5 members, although this is not currently a mandatory requirement. This is an area of interest to the ESFA and should be considered particularly as the trust grows in the next few years, and as the two individual members are also directors the aim of this is to ensure the members have sufficient separation from the Board so as to provide external oversight.

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
1	Roles and responsibilities It was noted that there is a lack of clarity over individuals' roles and responsibilities within the finance team particularly in respect of the accounting system, once the former finance manager had left the Trust.	HIGH	This caused omissions of some entries such as payroll entries, and duplication of others such as purchase invoice payments, and therefore a material misstatement of the figures. This also caused journal entries to be processed without clear audit trails.	It is recommended that clear roles and responsibilities are allocated amongst staff and clear procedures are put in place for all aspects of the accounting system. Adequate training must be given to all members of staff who are responsible for maintaining the accounting records.	Agreed. A monthly checklist will clarify responsibilities and ensure all accounting tasks are completed by month end. Roles and expectations will also be reviewed and training arranged as required. Training is planned for the end of January and further training will be organised as required Target date: 31 st Jan 2018
2	Cash management Bank reconciliations were not performed during the year. This has resulted in material adjustments being required as prompted by auditors. As this work is being done long after the date of transactions, there is increased risk of misstatement and does not reflect timely bookkeeping or management.	HIGH	Conducting regular bank reconciliations is regarded as a basic financial management tool. In the absence of this basic check, the Trust is unable to prove that the accounts and the financial information is correct.	It is recommended that formal bank reconciliations are performed on a regular basis - once a month - and the bank balance as per PS Financials is reconciled to the bank balance as per the bank statements. Any issues identified should be investigated and resolved on a timely basis.	Agreed. Bank accounts will be reconciled at least monthly and reconciling items investigated. The reconciliation will be independently reviewed by a member of the University Finance team. Target date: 31 st Jan 2018

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
3	Accounting system Through discussion with management, and review of the financial data presented for audit, it is apparent that those in charge of the finance function are not fully conversant in PS Financials and inadequate training was provided.	HIGH	For example, we note that some expenditure invoices have been posted multiple times to creditors and expenditure, following payment, we note that the transaction has been between bank and expenditure; therefore overstating expenditure and leaving the MAT open to risk of overpayment.	We recommend that all appropriate staff members are formally trained on PS Financials and are trained on their function as well as other functions to ensure that there is always someone on hand with knowledge of the system to advise appropriate treatment.	Agreed. Roles and expectations of staff responsible for maintaining accounting records will be reviewed. Training is planned for the end of January and further training will be organised as required (recommendation 1). In addition members of the University Finance team will be trained in the use of PS Financials and we will consider buying additional consultancy services from the software supplier to use when further support is required. Target date: 28 th Feb 2018
4	Management information It is clear from the information viewed, that full management information has not been prepared and reviewed on a regular basis during the year.	HIGH	Management have a responsibility to review regular management information and this would have identified the deficiencies in the system at an earlier point during the year.	A full set of management information should be made available and reviewed at least on a termly basis.	Agreed: Management accounts will be circulated to Management each month and a schedule of LGB, Committee and Trust board meetings will make it clear which month's management accounts go to each meeting. Management accounts will include a balance sheet and a section reconciling figure to the ledger. Target date: 28 th Feb 2018

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
5	Control accounts Control accounts are not being utilised properly, reviewed nor reconciled, such as net wages, PAYE/NI, pensions, trade debtors, trade creditors.	HIGH	The payroll charge is significant to the MAT - if the journals are not being processed monthly as per the payroll reports, then there is a major weakness in the controls surrounding the payroll function. There is therefore a risk of misappropriation of funds as the reporting could be manipulated and payments manipulated also as there is not a full reconciliation of the charge and the payments made.	We recommend that the payroll process is revised and a formal reconciliation of the payroll report with the postings as per the financial system are reconciled with the payments made. This should ensure that staff are paid appropriately as per approved calculations and that we reduce any misappropriation risks.	Agreed. A formal process will be put in place for the payroll to be signed off in line with the bank mandate before the payroll bacs are sent. Reconciliations will be completed monthly and be included on the monthly check list (recommendation 1). A formal process for recovery of overpayments will be put in place. Target date: 31 st Jan 2018
6	Supplier transactions The supplier ledger within PS Financials is not being utilised, and management have confirmed that they do not have a complete listing of liabilities as at 31 August 2017, with the year end position being ascertained based on post year end payment of physical invoices located.	HIGH	Given the size of the trust, the lack of a functioning supplier ledger increases the risk of duplicate payments being made as there is no complete trail of purchase invoices and payments made.	We recommend that supplier invoices and payments are properly tracked within the accounting system so that outstanding balances can be seen and historic invoices can be viewed.	Agreed. Payments to suppliers will only be made against invoices that have been entered on the accounting system. Outstanding and debit balances will be investigated and resolved monthly and statements will be obtained from key suppliers and reconciled at least every 3 months. Target date: 31 st Mar 2018

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
7	Land and Buildings As at 8 January 2018 a 125-year lease for the land and buildings of UAE was made available to us as the external auditors. Being dated in August 2016, this represents a material prior year adjustment to recognise the long leasehold property controlled by the Trust, and this information should have been made available to us during the prior year.	HIGH	Whilst the accounts have been adjusted for this material prior year adjustment, this is a significant item which we as auditors had not been initially informed of.	The Trust has a responsibility to ensure that there is no relevant audit information of which the external auditor is unaware.	We had already disclosed information regarding the lease to the auditors. We will obtain a professional valuation. Target date: 30 th Apr 2018
8	Unidentified provisions Upon querying the accruals balance, there is an unsupported general provision for energy costs of £111,000, and unidentified accruals of £42,325. Total energy costs recognised within expenditure for the year however only amounts to £58k.	HIGH	This indicates a lack of clarity and control over the expenditure recognised within the trust's financial statements.	We recommend that proper controls are put in place around supplier invoices which would allow clear monitoring of transactions.	Agreed. Payments to suppliers will only be made against invoices that have been entered on the accounting system. Outstanding and debit balances will be investigated and resolved monthly and statements will be obtained from key suppliers and reconciled at least every 3 months. (Recommendation 6). At year end the reasons for accruals will be clearly documented. Target date: 30 th Sept 2018

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
9	Related party transactions There is not an appropriate process in place whereby related parties and pecuniary interests of key management personnel are recorded on a timely basis	HIGH	There are specific ESFA requirements that state Academies are to keep a record of related parties and pecuniary interests of all key management personnel, directors and budget holders. This is to ensure that all goods and services procured are done so at a reasonable rate, and to ensure that management are fully aware of related parties at all times.	It is recommended that a formal register of related parties and pecuniary interests is kept centrally by the finance team. It is further recommended that this is updated when new staff are appointed, and on an annual basis. This will allow for the MAT to be aware of all related parties at all times.	There is a formal register of related parties maintained by the University Governance team.
10	Accruals based reporting The accounting records were being maintained on a cash accounting basis instead of an accruals and prepayments basis. A number of adjustments had to be processed to recognise the appropriate accruals, creditors and accrued income.	MEDIUM	There is a risk that incorrect financial information is presented to the board.	The finance staff need to be trained to understand the difference between cash accounting and the accruals concept. This should incorporate an understanding of cut off procedures making it easier to identify the necessary adjustments for monthly, termly and year end accounts.	Accounting records are maintained on an accruals basis. The monthly check list and actions in response to recommendation 6 and 8 will ensure that management and year end accounts are prepared on an accruals basis. Target date: 30 th Sept 2018

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
11	<p>VAT receivable</p> <p>Throughout the account period, we note that only 2 VAT 126 returns have been processed and submitted.</p> <p>The UTC VAT balance per PS Financials is £56k overstated compared to the draft claim workings.</p> <p>The VAT balances have not been reconciled during the period.</p>	MEDIUM	<p>There is a risk that these claims have been prepared incorrectly and/or the balance showing as receivable in the accounting system is incorrect.</p> <p>The Trust is also not taking advantage of cash flow opportunities as these returns can be processed on a monthly basis.</p>	<p>It is firstly recommended that the financial system is brought up to date and the VAT 126 returns already processed are reviewed for appropriateness. It is further recommended that the governors of the MAT consider adopting the policy of processing these returns on a monthly basis to aid inflows.</p>	<p>Agreed. VAT 126 returns will be prepared, reconciled to ledgers and sent to HMRC monthly. The monthly check list will evidence that this task has been completed.</p> <p>Target date: 31st Mar 2018.</p>
12	<p>Fixed asset register</p> <p>A formal fixed asset register is not maintained</p>	MEDIUM	<p>The figures within the trial balance in respect of fixed assets are highly material to the MAT, we were not provided with supporting documentation by way of a fixed asset register. This therefore a risk that depreciation, capital additions and capital disposals are not processed appropriately on a timely basis. The fact that this is not being done on a timely basis means that management may not remain aware of the true position of the Academy at all times.</p>	<p>It is recommended that a formal fixed asset register is maintained with capital transactions and depreciation being posted on a regular basis (at least termly), when the management accounts are prepared. This will ensure that the true position of the Academy is reflected at all times.</p>	<p>Agree. The register currently details IT equipment only. A full fixed asset register is being prepared. Fixed asset transactions and depreciation will be posted to the ledger monthly and reconciled to the fixed asset register.</p> <p>Target date: 31st Mar 2018.</p>

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
13	LGPS pensions We identified discrepancies between the amounts showing on the actuarial reports for employer contributions received, and the trust records of employer contributions paid to the scheme.	MEDIUM	These discrepancies indicate potential error in the information used by the actuaries in preparing the LGPS pension report figures.	We recommend that the Trust reviews the documentation received by the actuaries and reconciles contributions paid to internal records, with discrepancies investigated and resolved directly.	Agreed. Target date: 30 th Sept 2018.
14	Agency staff The agency staff costs in the year of £587k is extremely high compared to other trusts, and indicates a potential staffing and budgeting issue which should be closely monitored.	MEDIUM	Having heavy reliance on agency staff is a potential issue and needs to be managed by the team. Whilst there is an obvious financial impact, it also has an impact on the day to day operations as there is inconsistency in approaches as staff change.	We recommend that the Trust reviews its staffing position and prepares an action plan in respect of this area.	Agreed. A staff budget and recruitment strategy will be prepared as part of the 2018/19 budget process. Target date: 30 st June 2018.

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
15	Members and directors It was noted that the appointed members and trustee directors of the trust were not reflected accurately and on a timely basis at the get-information-schools.service.gov.uk website (previously known as Edubase) - (the DfE's register of educational establishments).	MEDIUM	The Trust is in breach of the Academy Handbook requirement that the Trust must notify DfE of the appointment or vacating of the positions of members, directors and local governors within 14 days of that change through the governance section of DfE's Edubase.	We recommend that the Trust gets the information up to date and monitors this on a regular basis.	Agreed. We are in the process of updating the register to reflect the current position. We will update the register to show the new directors and governors. Target date: 31st January 2018.
16	Expenditure vs budgets The budget for the year (as approved by Governors) had not been uploaded onto the PS Financials system. Therefore, the current financial position cannot be properly monitored or managed as compared to the budgets set.	LOW	Expenditure cannot be monitored against the budget without accurate reporting and there is therefore an increased risk of the Trust not adhering to the approved budget which increases the risk of excess spending.	The approved budgets are uploaded into PS Financials once finalised. It is further recommended that the budget to actuals are compared on a regular basis (perhaps termly) and any projected under / over spends can be brought to attention in a timely manner.	Agreed. Budgets will be loaded onto PS financials. Management accounts will be circulated to Management each month (recommendation 4) with variances to budget investigated and explained in the commentary. Target date: 28 th Feb 2018.

Section 3: Operation of the Accounting and Internal Control Systems

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE
17	Payroll records As a result of the testing performed, an instance was noted where we could not locate a staff leaver's supporting documentation to confirm their leave date from UAE.	LOW	There is a risk of misappropriation of the MAT's funds here as incomplete record keeping could result in this member of staff not being removed from payroll appropriately.	It is recommended that the process of processing starters and leavers is formalised. As well as this, there should be a checklist for starters / leavers to ensure that the appropriate steps are taken and documents are processed; for example a P45 and resignation letter.	Agreed. A formal process for checking starters, leavers and variations will be put in place and signed off before the payroll is finalised. A formal process will be put in place for the payroll to be signed off in line with the bank mandate before the payroll bacs are sent (recommendation 5). Target date: 28 th Feb 2018.
18	Central recharges Where internal bank transfers are made, there is not always supporting documentation available.	LOW	If inter academy transactions are not being consistently monitored and recorded, then the risk of entity level reporting being inaccurate is increased.	Where a financial transaction is to be processed there should be sufficient and appropriate evidence and documentation to support this. Where there are internal recharges required to be posted via journal, it is recommended that a schedule is maintained as to the basis of the recharge as well as who it has been approved by and when the posting has been made.	Agreed. Supporting documentation will be checked before any accounting entries are made, including receipts, payments and journals. The completion of regular internal recharges will be included on the monthly check list (recommendation 1) and bank reconciliations completed and reviewed monthly (recommendation 2). Intercompany balances will be reconciled monthly and the Trust will consider reducing the number of bank accounts from 3 to 1 to simplify the accounting entries. Target date: 28 th Feb 2018

Section 3: Operation of the Accounting and Internal Control Systems

We have given each of our observations a risk rating as explained in the key below:-

RISK RATING FOR MANAGEMENT REPORT POINTS		
	Risk rating	Explanation
	Low	Issues that would, if corrected, improve the internal controls or accounting practices in general but are not vital to the overall system. These are generally issues of best practice that we feel would benefit you if you introduced them.
	Medium	Issues that have an important effect on internal controls but do not need immediate action. You may still meet a system objective in full or in part or reduce (mitigate) a risk adequately but the weakness remains in the system.
	High	Issues that are fundamental and material to your system of internal control. We believe that these issues might mean that you do not meet a system objective or reduce (mitigate) a risk.

Section 5: Sector Update

Prior Year Points

	MATTER ARISING	RISK	IMPLICATION	RECOMMENDATION	MANAGEMENT RESPONSE	2017 FOLLOW UP
1	Accruals We note an accrual for £34k has been made for Southwark heating and an accrual of £44k for IT services from RM. We have noted the calculations to support these, but understand 3rd party evidence (an invoice, for example) is not available.	MEDIUM	Accruals may be overstated.	To ensure that all accruals are supported by evidence of invoices where possible.	The Academy is aware that there are costs involved with the heating supplied by Southwark Heating and also the IT services supplied by RM Education. Despite requests we have not received any invoices. It is however prudent to accrue for these costs.	Unfortunately we do not believe this has been addressed as the financial information that was presented for audit had not been prepared on an accruals basis - this has therefore been repeated as an issue in the current year.
2	Bank reconciliations Bank reconciliations are not being signed off as reviewed.	LOW	There is a risk that reconciliations are not being performed adequately and/or in good time.	Sign off bank reconciliations once reviewed; consider the possibility of a dual review or a separate reviewer to the person posting income and expenditure.	Bank Reconciliations will now be prepared by the Finance Officer in each school and signed by the Trust Business Manager.	Again, this issue has not been seen to be resolved by management for the 2016/17 financial year and this issue has been repeated in the current year.

Section 5: Sector Update

Academies Useful Links

There are a number of links which the Governors and senior leadership might find useful and these are listed below:-

Gov.uk

<https://www.gov.uk/government/collections/schools-financial-health-and-efficiency>

<https://www.gov.uk/guidance/schools-financial-efficiency-top-10-planning-checks-for-governors>

<https://www.gov.uk/academies-fianncial-assurance>

<https://www.gov.uk/academies-severance-payments>

<https://www.gov.uk/government/collections/academies-investigation-reports>

NABSM good practice Library:

<http://nasbm.co.uk/Home/Efa-Academies-Library.aspx>

FD Forum:

www.thefdforum.co.uk

ICAEW:

www.icaewvolunteers.com

Section 5: Sector Update

Academies Financial Handbook 2017

The 2017 Handbook came into force on 1 September 2017. The annually updated academies financial handbook is a key document that sets out the financial framework for academy trusts, and compliance with the handbook is a requirement of your funding agreement with the Secretary of State.

There is no substitute for reading and making reference to the handbook directly. It sets out requirements which the trust must comply with, as well as recommended best practice.

A few points to note are as follows:

- Academy trusts must publish on their website up to date details of its governance arrangements. This includes:
 - The structure and remit of the members and board of directors
 - For each member who served at any point over the past 12 months, their full names, dates of appointment/resignation and relevant business and pecuniary interests including governance roles in other educational institutions.
 - For each trustee who served at any point over the past 12 months, the same information above for members plus also their term of office and attendance records at board meetings over the last academic year.

Register of interests must capture relevant business and pecuniary interest of members, directors and also any senior employees to aid the trust in managing its relationships with any connected

parties to avoid both real and also perceived potential conflicts of interest.

- Academy trusts must notify DfE of the appointment or vacating of the position of any:
 - Member
 - Trustee
 - Local governor
 - Chair of trustees/directors
 - Chair of local governing bodies
 - Accounting officer
 - Chief financial officer

Including direct contact details, within 14 days of that change.

Notification must be made through the governance section of DfE's <https://get-information-schools.service.gov.uk> which is accessed via the Secure Access Portal.

- ESFA's accounting officer will send a 'Dear Accounting Officer' letter annually to all academy trust accounting officers, covering issues pertinent to their role such as developments in the accountability framework and findings from ESFA's work with trusts.

Accounting officers must share this letter with their members, directors, chief financial officer and other members of the senior leadership team, arrange for it to be discussed by the board of directors and take action where appropriate to strengthen the trust's financial systems and controls.

Section 5: Sector Update

Revised Governance Handbook

In January 2017, the Department for Education published the new version of its Governance Handbook for trustees/directors of academy trusts.

All boards, no matter what type of schools or how many schools they govern, have three core functions:

1. Ensuring clarity of vision, ethos and strategic direction;
2. Holding executive leaders to account for the educational performance of the organisation and its pupils, and the performance management of staff; and
3. Overseeing the financial performance of the organisation and making sure its money is well spent.

Effective governance is based on six key features:

- **Strategic leadership** that sets and champions vision, ethos and strategy.
- **Accountability** that drives up educational standards and financial performance. 9
- **People** with the right skills, experience, qualities and capacity.
- **Structures** that reinforce clearly defined roles and responsibilities.
- **Compliance** with statutory and contractual requirements.
- **Evaluation** to monitor and improve the quality and impact of governance.

The first two features are the core pillars of the board's role and purpose. The second two are about the way in which governance is organised, and the last two are about ensuring and improving the quality of governance.

The full Code can be found at

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/582868/Governance_Handbook_-_January_2017.pdf

Section 5: Sector Update

Employment tax changes commencing 6 April 2018

From April 2018, the employment tax rules are changing again. It is crucial that all employers are aware of these changes and consider the impact they may have on their internal procedures and controls and any necessary communication with employees.

Salary sacrifice Schemes

From April 2017, it was no longer possible to implement a salary sacrifice scheme unless the benefit being provided under the scheme fell within one of the excluded categories of:

- Childcare benefits
- Pension contributions
- Employer-provided pension advice
- Cycle to work schemes
- Ultra-low emission cars (<75 g/km)

If employers had other schemes in place, such as for employer provided training or the provision of mobile phones which commenced before 6 April 2017 then, under transitional rules, these are not subject to these rules until 6 April 2018 - so a review of schemes in place is needed before this date.

The transitional rules are extended until April 2021 where the benefit being provided is a company car (>75 g/km), the provision of accommodation or subsidised school fees.

If you are contractually obliged to continue to provide benefits under salary sacrifice schemes which are not within the excluded categories or within

the transitional rules, the amount of salary foregone by the employee will remain taxable even though they are not being paid this amount.

Employers need to understand their payroll obligations before the April 2018 deadline when the first set of transitional rules expire as otherwise they risk under-deducting tax from their payroll from April 2018 onwards.

Pension Automatic Enrolment

Under Automatic Enrolment all employers will have to provide a workplace pension for eligible staff by 6 April 2018 and many already do. On that date both the minimum employee and minimum employer contributions will increase and then again in April 2019.

	Minimum employer contribution	Minimum employee contribution	Total minimum contribution
Now	1%	1%	2%
From April 2018	2%	3%	5%
From April 2019	3%	5%	8%

Both the employer and employee can choose to contribute greater amounts to the pension if they wish; however, it is the employer's responsibility to ensure the schemes are inline with the minimum contributions.

With the cost of pension contributions for employees set to rise fivefold, employers should consider implementing a salary sacrifice scheme for the employee element whereby the employee gives up part of their salary and the employer pays this straight into the pension.

Section 5: Sector Update

The General Data Protection Regulations

Data protection legislation exists to protect the public and uphold their right to privacy and freedom. The rapid growth in digital technology and the potential for cyber attack has created a need to review the way information is collected, used, shared and stored. The General Data Protection Regulation (GDPR) which becomes UK Law on 25 May 2018 sets out to create the framework for the future of privacy legislation and has far reaching consequences for all organisations, including fundraising charities.

GDPR will affect those organisations that handle the personal data of customers, supporters or members, referred to as 'data subjects'. Data subjects have many new rights under GDPR such as the right to be forgotten, the right to object and the right to compensation. Organisations will need to be able to demonstrate they have an understanding of the regulation and the ability to comply with data subject requests. The need to demonstrate compliance with GDPR is paramount for most organisations for three main reasons:

1. Reputational damage – The public have developed a heightened level of sensitivity when it comes to their personal data. Breaches of data protection in the future will be high profile, the public will be encouraged to seek demonstrable evidence organisations are protecting them.
2. Substantial financial penalties – The Information Commissioner's Office (ICO) has new powers to warn, reprimand and fine organisations up to €20m (Most likely to become pounds sterling) for breaches of GDPR.

The biggest fines will be reserved for breaches of the most basic of rules such as the right to consent to marketing.

3. Liability to data subject – Article 80/82 of GDPR gives data subjects the right to judicial remedy for the first time. Subjects will be able to sue for material and non-material loss.

The main discussion for charitable entities revolves around permission to contact individuals. There are six conditions for processing personal data, but only three that really apply to not for profit entities.

1. Necessary for Contract

If you have sold a supporter something, as apposed to accepting a donation, you can communicate with them because of the contract and the need to legally fulfil that arrangement. They have the right to complain and have legal recourse should you not fulfil your commitment to them.

2. Consent

Widely understood and definitely the best condition of the six. It must be given unambiguously, freely, in an informed way, specifically and you must be able to demonstrate you have it. Silence is effectively an opt-out. Consent does not lapse, so once you have it you don't need to renew although good practice suggests the value of refreshing consent, and it is important to have a robust policy for the length of time you hold personal data. Only if a supporter opts-out should there be no further communication with them.

Section 5: Sector Update

Consent will be specific to a particular channel and a particular purpose, and charities need to make sure they record how they are communicating and flag specific consents accordingly.

3. Legitimate interest

The Legitimate interest condition is a charity's interest to achieve an objective. For example, it is in a charity's legitimate interest to raise important funds to continue its work. If consent hasn't been given in advance of processing personal data, this might be a charity's only option.

For example, it can be used to write to people (printed letter) with whom the charity doesn't yet have consent to communicate. If a supporter hasn't indicated they don't want a telephone call and aren't registered with TPS, it can be in a charity's legitimate interest to telephone them.

While using Consent or Legitimate interest, it is important to offer supporters the opportunity to Opt-out of printed communications or telephone calls at every engagement. A simple, easily understood privacy notice printed in every direct mail pack or newsletter for example will ensure this is clear and the supporter is being treated fairly and in accordance with data protection.

For further information about demonstrating data protection compliance, data management audits and best practice, please contact Dan Fletcher of Kingston Smith Fundraising and Management dfletcher@ks.co.uk

Appendix 1: Corrected Misstatements and Reclassifications

As discussed in Section 2, whilst our assistance was required to help management get to an auditable trial balance position, the ETB as presented on 21 December has been taken to be the final draft position presented by management for audit. On this basis, the following corrected misstatements were made to this ETB:

	Balance sheet		SOFA		Effect on surplus/ (deficit) £000s	
	Dr £000s	Cr £000s	Dr £000s	Cr £000s		
	Initial surplus as per client ETB as at 21 December 2017				377	
1	Pension costs	-	-	19	-	(19)
	Actuarial gain	-	-	-	2	2
	LGPS pension creditor	-	17	-	-	-
	Being the adjustments to recognise UTC LGPS movement					
2	Governance costs	-	-	15	-	(15)
	Accruals	-	15	-	-	-
	Being accrual for additional Kingston Smith fees incurred to support the year end process					
3	Furniture and Equipment additions	49	-	-	-	-
	Computer additions	92	-	-	-	-
	Building improvements	17	-	-	-	-
	Premises costs	-	-	-	158	158
	Being capitalisation of fixed assets processed as revenue costs					

Appendix 1: Corrected Misstatements and Reclassifications

		Balance sheet		SOFA		Effect on surplus/ (deficit) £000s
		Dr	Cr	Dr	Cr	
		£000s	£000s	£000s	£000s	
4	Depreciation charge	-	-	42	-	(42)
	Furniture and Equipment depreciation	-	10	-	-	-
	Computer depreciation	-	31	-	-	-
	Building improvements depreciation	-	1	-	-	-
	Being depreciation charge on capitalised fixed asset additions					
5	Accruals	35	-	-	-	-
	Depreciation charge	-	-	-	35	35
	Being removal of the duplicated depreciation expense per client					
6	Salary costs	-	-	92	-	(92)
	Donated salary income	-	-	-	92	92
	Being recognition of CEO salary donated from LSBU					
7	Pension costs	-	-	4	-	(4)
	LGPS pension creditor	-	4	-	-	-
	Being the adjustments to recognise the MAT LGPS movement					

Appendix 1: Corrected Misstatements and Reclassifications

		Balance sheet		SOFA		Effect on surplus/
		Dr	Cr	Dr	Cr	(deficit)
		£000s	£000s	£000s	£000s	£000s
8	Long leasehold fixed assets	23,000	-	-	-	-
	Fixed asset reserve brought forward	-	23,000	-	-	-
	Being prior year adjustment to recognise the UAE long leasehold					
9	Depreciation charge	-	-	184	-	(184)
	Long leasehold fixed asset depreciation	-	184	-	-	-
	Being current year depreciation charge on long leasehold UAE premises					
	Revised surplus as per final financial statements					308

Appendix 2: Uncorrected Misstatements and Reclassifications

		Balance sheet		SOFA		Effect on surplus/ (deficit) £000s
		Dr	Cr	Dr	Cr	
		£000s	£000s	£000s	£000s	
1	Unconfirmed	-	-	55	-	(55)
	VAT recoverable	-	55	-	-	-
	Being the adjustments to recognise UTC LGPS movement					
2	Governance	-	-	12	-	(12)
	Unconfirmed	-	-	-	12	12
	Being Kingston Smith fees included within accruals but not expenditure					
3	Energy	-	-	43	-	(43)
	Unconfirmed	-	-	-	43	43
	Being energy accrual made in excess of energy costs recognised					
4	Accruals	31	-	-	-	-
	Unconfirmed	-	-	-	31	31
	Being release of unidentified UAE accruals					

Appendix 2: Uncorrected Misstatements and Reclassifications

		Balance sheet		SOFA		Effect on surplus/ (deficit) £000s
		Dr	Cr	Dr	Cr	
		£000s	£000s	£000s	£000s	
5	Accruals	42	-	-	-	-
	Unconfirmed	-	-	-	42	42
	Being release of unidentified UTC accruals					
6	Unconfirmed	-	-	20	-	(20)
	Trade creditors	-	20	-	-	-
	Being UTC unrecognised trade creditors					
	Net potential effect of unadjusted misstatements and reclassifications					(2)

Appendix 3: Other Matters

Engagement & Independence

Our engagement objective was the audit of the South Bank Academies.

We have implemented policies and procedures to meet the requirements of the Financial Reporting Council's (FRC) Ethical Standards. To this end we considered our independence and objectivity in respect of the audit for the period under review before commencing planning our audit and communicated with you on these matters in our pre-audit letter dated 9 June 2017.

No other matters have come to our attention during the audit which we are required to communicate to you and the safeguards adopted were as described in our pre-audit letter.

Qualitative aspects of accounting practices, accounting policies and financial reporting

Based on our audit work performed, we believe that the Strategic Report, Trustee's Report and financial statements for the period under review comply with United Kingdom Accounting Standards and the Companies Act 2006.

During the course of our audit of the financial statements for the period under review we did not identify any inappropriate accounting policies or practices.

Matters specifically required by other Auditing Standards to be communicated to those charged with governance

Other than as already explained in our Engagement Letter, Pre-Audit Letter and this Post-Audit Management Report, there are no other specific matters to communicate as a result of our audit of the financial statements under review.

	CONFIDENTIAL
Paper title:	Report on UK Visas and Immigration (UKVI) Issues affecting the Tier 2 License
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Mandy Eddolls, Executive Director of HR Ed Spacey, Head of HR Business Services
Executive/Operations sponsor:	Mandy Eddolls, Executive Director of HR
Purpose:	To update Audit Committee
Recommendation:	The committee is requested to note this report.

1.0 Background

- 1.1 UK Visas and Immigration require us to keep strict controls on the number of hours migrants work, and there are extensive and detailed documents which have to be kept about each person, and checks which have to be carried out.
- 1.2 In September 2017, two students on Tier 4 Visas were found to have worked more than the maximum 20 hours per week permitted by their visa. They were both postgraduates, one worked 20.5 hours during one week, the other 37 hours during one week.
- 1.3 The students were unclear about how the regulations applied between term and non-term time, and internal processes were not advanced enough to prevent this.
- 1.4 The University obtained external legal advice, interviewed the 2 students and made a required report to the Home Office.

2.0 Implications

The effect of reporting the above means:

- An announced inspection by the Home Office is possible, though we have heard nothing to date.
- There may be a civil penalty for LSBU (estimated to be a warning-based on information from Penningtons Solicitors).

The Home Office reserve the right to withdraw the 2 students permission to stay,

but this is highly unlikely, based on the legal advice received and mitigation supplied.

We have had no contact from UKVI since reporting.

- 2.1 Any Home Office inspection of our UKVI processes is important, as they retain the ultimate right to downgrade our license and issue an action plan of improvement, or remove our licenses to sponsor international workers.
- 2.2 Based on the external legal advice obtained, the above penalties are highly unlikely.
- 2.3 However, any future reported breaches which occur after any Home Office review, are likely to be treated punitively. Therefore, it is vital that processes and systems are improved, and this is being done as outlined in section 4.0

3.0 Outcome of file review by Immigration Lawyers

- 3.1 Penningtons Solicitors will be supporting LSBU throughout any inspection by the Home Office. They have already been working with the International Office and People & Organisation, and made some initial recommendations about files – letter attached for information.
- 3.2 Their principal recommendations (attached) concerned our use of the Resident Market Labour Test (proof that the skills are not widely available within the UK) and the tie up of the Standard Occupational Classification Codes and our Certificates of Sponsorship. All their recommendations have been implemented.
- 3.3 They further commented that the general files were poor and, whilst they could find no additional breach that we needed to report, the systems for filing important documents was not secure.
- 3.4 Following this comment from Penningtons, extensive work has been undertaken to improve the methodologies for retaining key information.

Eversheds Solicitors have also carried out some wider general training/review across People and Organisation.

- 3.5 Key findings from a review of historical files by Eversheds Solicitors:
 - 46 file packs reviewed. 20 required further amendments.
 - 9 Certificate of Sponsorship file packs examined (Tier 2 visas) of which 6 could be improved prior to Home Office inspection.
 - Right to Work checks have in the past been delegated to recruiting managers, with poor results. This work is now centralised into the HR team.
 - Recommendation to have quarterly file audits.
 - Recommendation to run regular refresher training for staff.

All actions recommended by the solicitors are being, or have already been,

actioned.

4.0 Process Improvements

Arrangements for managing UKVI are being changed and significant progress made. Measures include:

- A new Authorising Officer (senior responsible person) and an operational lead have been appointed to manage the process centrally, working closely with the International Office.
- A new 'Student Employees – Policy and Procedure for Tier 4 Workers' has been approved and implemented.
- Immediate changes made to the process for monitoring hours to be worked in advance - focusing on a maximum of 20 hours. A further new process mapping document is being developed by 3 November.
- Briefing on regulations to Deans in Schools with the highest volume of migrant workers, and managers of all staff on visas completed in November 2017.
- Reviewing and developing improved online Tier 2 and Tier 4 staff training.
- New process already implemented for Right to Work checks of Ambassadors – now undertaken at Assessment Centre stage, and operated by the Recruitment Team.
- Major file review across People & Organisation addressing points raised by solicitors: all files of all employees hired since 2008 is currently in progress.
- Tier 4 files continue to be reviewed across the International Office.

5.0 Summary

5.1 The actual breach was minor and looks increasingly like it will not prompt any action from UKVI.

5.2 The audits completed both by Penningtons and then subsequently by Eversheds highlighted areas that needed improvements if we were to face an audit – which could happen at any time and without reason – by UKVI.

5.3 Significant work has been done since the audits have been completed and progress with implementing all recommendations has been made.

This page is intentionally left blank



LONDON

Private and Confidential
London South Bank University
Kate Burrell
Head of Policy
kate.burrell@lsbu.ac.uk

T: +44 (0)20 7457 3000
F: +44 (0)20 7457 3240
DX:42605 Cheapside
Penningtons Manches LLP 125
Wood Street
London
EC2V7AW
United Kingdom
www.penningtons.co.uk

By email only

29 September 2017

Dear Kate

Tier 2 findings -27 September 2017

We undertook a review of a small sample of Tier 2 files on 27 September 2017 in preparation for a possible UKVI audit. We have made general comments in relation to points we have discussed. We have also made individual comments in relation to the files reviewed.

Although improvements continue to be made, as can be seen, there are many common issues and some of them can be easily rectified as the documentation is possibly on the main HR file or can be requested from the individual. Therefore, we suggest that the files are once again checked to ensure that the missing information, where possible, is obtained and put on the UKVI file.

General comments

Spreadsheet

Please ensure that you are able to provide to the UKVI a spreadsheet of all employees (if requested). The spreadsheet should include:

- Name, nationality, visa type and visa expiry date

For auditing purposes, please also run a report which lists visa start date and LSBU start date so you can check that you have visas covering the whole period that each migrant has worked for yourselves. Some individuals may have multiple visas.

I understand that a report is run every month which flags everyone who has a visa expiring in the next three months so they can be contacted. Please ensure that you can provide this to the UKVI if requested.

History of contact details

From August 2017, I understand that LSBU has had a self-service system for individuals to update their contact details. This system also keeps a history of their contact details.

3103503/66236006v1

LONDON • BASINGSTOKE • CAMBRIDGE • GUILDFORD • OXFORD • READING • SAN FRANCISCO

Penningtons Manches LLP is a limited liability partnership registered in England and Wales with registered number OC311575. It is authorised and regulated by the Solicitors Regulation Authority. A list of the members of Penningtons Manches LLP is open to inspection at its registered office, 125 Wood Street, London EC2V 7AW. Any reference to a partner in relation to Penningtons Manches LLP means a member of Penningtons Manches LLP. San Francisco is an office of Penningtons Manches (California) LLP, a California registered limited liability partnership v.ith number 202016025001, registered in England and Wales with registered number OC396811.

Please ensure that at least once a year a reminder is sent out to all Tier 2 migrants (or all employees) to remind them to update their details.

Please make sure all Tier 2 migrants have a UK address, landline and mobile phone number recorded on the HR system.

Possible interview of Tier 2 migrants

As discussed, it is possible that the UKVI might wish to interview Tier 2 migrants as part of an audit. They often provide prior notice if they wish to conduct these interviews. Therefore, we would suggest that you add information in relation to this to the information sheet that is already given to Tier 2 migrants on an annual basis regarding their responsibilities as a Tier 2 migrant. Please let us know if you would like us to review this information .

Prevention of illegal working checks

I understand that all checks will be centralised from 21 October 2017. Therefore, there should be greater control with Student Ambassadors and Hourly Paid Lecturers as these were previously checked within the schools. Please ensure work restrictions are carefully checked and the necessary safety checks are put in place were necessary to ensure no one breaches their conditions of work.

20 hour work limit

I understand that a decision has been made within the University that PhD and master students will only be allowed to work 20 hours per week regardless of if it is term time or not. This should minimise the risk of students working over their allocated hours because of uncertainty over if it is term time or not.

In addition, HR will check all booked hours for students before the work commences, this list will then be sent to the international student team so they can check if any individuals are Tier 4 visa holders. Only after this double check will sign off be given for student to undertake the work. Payroll will also be doing a third check. However, LSBU realise that by this stage, if the student has worked over their allocated hours then a breach would have already occurred.

Although this might be time consuming, this is a robust strategy which, if carried out as outlined, should prevent students working more than their allowed hours at the University.

Supplementary work

Please ensure that Tier 2 sponsored migrants who also have contracts to undertake supplementary work e.g. as hourly paid lecturers, are working in line with the supplementary guidelines. As per the Tier 2 Sponsor Guidance paragraph 38.50 supplementary employment must:

- *"be in the same profession and at the same professional/eve/ as the work for which the migrant's CoS was assigned or be a job which is in a shortage occupation listed in Appendix K of the Immigration Rules-- if the occupation is later removed from the list of shortage occupations, the migrant must finish that employment*
- *be for no more than 20 hours a week*
- *be outside of the normal working hours for which the migrant's CoS was assigned"*

Please remember that someone must be monitoring this to ensure compliance. Therefore, please implement a process whereby supplementary work is also checked to ensure it is in line with the above before the work is carried out by Tier 2 migrants.

Copies of visas/BRPs

Some visa/BRP copies were very hard to read. Please ensure copies/scans taken are clear and all the information can be easily read.

Absences

I understand that from August 2017 the monitoring of absences has become centralised. Therefore, going forward, HR can see if someone is sick, on annual leave etc. Please ensure that there is a clear process on who is reporting into HR if a Tier 2 migrant doesn't show up to work. There should also be a second point of contact to undertake this job if that person is away e.g. on annual leave/sick.

Generally, the system as it stands now often shows that a migrant has not had any annual leave during the last 12 months (or very little) presumably because this has been recorded in each department. However, going forward, if it is all booked through the HR system then this problem should be resolved.

In terms of preparing for an audit we would recommend that you obtain information in relation to the days that the current Tier 2 migrants have been absent in accordance with Appendix D.

Key Personnel

I understand that a request has already been made to change the AO and Key Contact. I also understand that the Level 1 and Level 2 user list is up-to-date.

I understand that the AOs (old and new) are aware of their added responsibility regarding checking CoSs assigned to migrants monthly and that this is happening.

Comments and action points regarding Tier 2 files reviewed

██████████

- Academic reference from the University of Reading regarding her PhD was missing
- Internal spreadsheet lists her job title as "Hourly Paid Lecturer" not as per CoS/Contract. This should be changed. In addition, please see comments regarding supplementary work.
- Missing landline and mobile phone number
- SOC code missing, please print and put on file
- Right to work check was taken late

██████████

- Full CoS not on file. Once placed on file, please also check work location on the CoS as I understand from the file that she is working in your offices in Cambridge. Please also check that the Cambridge location was included as an address in your initial sponsor licence application or has been added as an additional site to the Sponsor licence
- Copy of migrant's qualifications not on file, please obtain
- SOC code missing, please print and put on file
- Employment contract not signed – please put signed copy on the

██████████

- CoS should have stated the reference number for both job adverts
- Advertising- Jobs.ac.uk- no screen shots, just confirmation that the advert was placed. If jobs.ac.uk can also confirm the contents of the advert this would be

beneficial. Note: even if they are able to do this it would not meet Appendix D but it would support the fact that this was a genuine recruitment exercise.

- Advertising – LSBU -the advert was printed off months after the advert had closed. If a screen shot was taken when the advert first appeared or while it was live, please place on the file.
- Notes on the file indicated that four individuals were shortlisted for interview. However, their CV/applications were not of file. In addition, for those EEA nationals shortlisted, the notes from the interview should be on file with reasons why they were not employed. I note that this is a PhD level post and therefore the most suitable candidate can be chosen.

- The individual switched from Tier 4 into Tier 2 and started the full-time job before the Tier 2 visa was approved. This is allowed, however you must have evidence that the CoS has been assigned and the migrant has submitted their Leave to Remain application before they can start the full time permanent post. Please try to obtain this information and place on file
- CoS was assigned for three years, but the contract is only for two years. I understand that LSBU is already aware of this issue.
- The back of the BRP is missing, please obtain
- Missing phone numbers, please obtain

- Start date on the CoS was recorded as 1/4/17 (a Saturday). The individual's contract and actual start date was the Monday (3/4/17). When there is a delay in start date it must be reported on the SMS within 10 working days. Even though this was late, please report on the SMS now. Please make sure going forward that the actual date stated on the CoS is in line with when the individual is due to start.
- Qualifications and evidence of experience missing, please obtain
- Advertising - Jobs.ac.uk - no screen shots, just confirmation that the advert was placed. If jobs.ac.uk can also confirm the contents of the advert this would be beneficial. Note: even if found it would not meet Appendix D but it would support the fact that this was a genuine recruitment exercise.
- Advertising – LSBU -the main advert didn't include all the relevant information e.g. salary, location, full job description. This could only be found by clicking through. When this is the case, then screen shots need to also be taken of the click through so the full advert can be seen. The click through advert on file was an internal view
- Advert stated that the individual should have "membership of relevant professional body". There was no evidence of this on the file, therefore please find and place on file.
- Please note that there was some information in relation to Washad stapled to the back of this individual's contract- please re file.
- Copy of Tier 2 visa not signed and dated.

- Job title on spreadsheet was listed as "hourly paid lecturer". I presume that this is for supplementary work, please check with CoS and change as necessary
- CoS missing from file- please print off and include
- SOC code missing -please print off and put on file

- Passport has expired - please obtain copy of current passport
- Contract has expired- please put current contract (and old ones if they relate to time as a Tier 2 migrant) on the file
- No job description on file, please print off and include
- Back of BRP not dated

██████████

- CoS start date is recorded as 1/2/17. Their application was not approved until 3/4/17 and the contracted start date was 18/4/17. Please ensure that the delayed start date has been reported on the SMS.
- Missing qualifications and experience
- Points scored regarding those shortlisted were on the file but the file was missing CV's /applications forms etc for those shortlisted and notes from the interviews regarding those shortlisted and the reasons why the resident workers were not employed. I note that this is a PhD role and therefore the best candidate can be chosen.
- Advertising - Jobs.ac.uk- no screen shots, just confirmation that the advert was placed. If jobs.ac.uk can confirm the contents of the advert this would be beneficial. Note: even if they can do this it would not meet Appendix D but it would support the fact that this was a genuine recruitment exercise.

Comments in relation to the Tier 2 spreadsheet

- There are some individuals on the spreadsheet which have expected end dates well before their visa end date. These files need to be closely monitored to ensure a report is made on the SMS if they do finish their role earlier than their CoS end date.

Comments regarding the prevention of illegal working files

From the files reviewed, we noted the following:

- ██████████ - back of BPR missing, passport not dated, previous visa not on file
- ██████████ - visa on file was a spouse visa not Family member of an EEA national as mentioned on the spreadsheet - please update
- ██████████ - back of BRP not dated, previous visas not on file- please obtain copies if possible
- ██████████ - visa not signed and dated

If possible, please obtain the missing information. We understand that copies of visas and passports previously taken have not always been signed and dated. However, where we have mentioned missing information please try to obtain it.

Conclusion

We would recommend visiting again and checking a different sample of files once the files have been rechecked.

I hope the above comments and action points are clear. If you have any questions please contact me or Hazar El-Chama

Yours sincerely

Penny Evans
Associate Director

	CONFIDENTIAL
Paper title:	Copyright and Licensing Agency audit
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Irina Bernstein
Executive/Operations sponsor:	James Stevenson
Purpose:	Information
Recommendation:	The meeting is requested to note good practice

Executive Summary

On 7th December 2017, the Copyright and Licensing Agency carried out a compliance audit to ensure LSBU's compliance with the terms of the CLA licence.

Overall compliance of LSBU is Good with many Excellent elements (the results of the audit are on page 5 of the audit report). We consider the recommendations to be 'light' and have started working on the implementation of the actions already. This should be easily achievable within the prescribed timelines.

This page is intentionally left blank

General Overview

Information about the Institution

Number of students (approx): 11,763 Full Time Equivalent Students (FTES)
 Membership: UUK/GuildHE
 Virtual Learning Environment: Moodle
 Reading List Software: Talis Aspire
 Digitisation Workflow Tool: Talis Aspire Digitised Content

CLA Auditor

Julie Murray – Education Licences Manager

HEI Representatives

Irina Bernstein – Licence Co-ordinator and Legal Services
 Martin Clark – Print Room Manager
 Steve Bowman – Senior Information Advisor (Health School)
 Malcolm Polfreman – Acquisitions and Subscriptions Team Manager
 Alison Chojna – Head of Library and Learning Resources
 Alan Doherty – University Library Site Manager
 Antonia Goodyer – Legal Services
 James Stephenson – University Secretary

Courses Audited

Course Title	Code
Curriculum Perspectives	TBE_7_003
Public Law	PGD_7_PUL
International Employment Relations	BBM_7_IER
Convergent Media Frameworks	AME_4_CMF
Civil Justice Contexts, Theories and Challenges	LAW_7_CVJ
What is Education?	EDU_4_EDS
Politics and Protest	DSS_6_PAP
Life sciences and medicines management	NCH_5_002
Psychopharmacology	PSY_6_PYP
Caring for Children and Young People with Life-Limiting Conditions	WHS_6_824

Introduction

As part of CLA's Higher Education Audit programme, London South Bank University was randomly selected for a Compliance Audit by CLA. The Audit visit was conducted under Clause 8 of The Copyright Licensing Agency Ltd Higher Education Licence on 7 December 2017. The primary purpose of the Audit was to ensure compliance with the terms and conditions of this Agreement, in

particular, but without limitation, with the provisions of clauses 3 (extent limits) and 4 (creation and storage of Digital Copies and access thereto) and by monitoring the observance of the moral rights of authors.

In addition, it was also an opportunity for CLA to learn more about how the Licence is being used in the Higher Education sector and to identify areas of good practice at the HEI.

The Audit comprised of two activities to assess the compliance of the HEI:

- Interviews with key representatives
- Review of content on the VLE

Findings

1) Policy, Procedure and Training and Communication—Implementation Framework

	Control	Evidence	Action
1.1	There is clear ownership and responsibility for the CLA Licence and Copyright	<ul style="list-style-type: none"> • All documentation related to the licence makes clear the central point of contact should staff have any questions. 	<ul style="list-style-type: none"> • No actions
1.2	Copyright guidance and/or policy is available to staff including information on the CLA Licence	<ul style="list-style-type: none"> • A clear and concise policy has been developed, together with guidance on the wider copyright landscape. This is available on the university's intranet. Throughout the documentation references are made to key aspects of the licence, such as repertoire, ownership, extent limits and the moral rights of the creator. 	<ul style="list-style-type: none"> • The guidance should be reviewed so that there is no confusion as to how scanning is conducted at LSBU. As the HEI operates a central scanning system, references to logging copies on a DCRF for instance should be removed. • A reference to the CLA photocopying and scanning licence in '<i>what copyright licences do we have?</i>' should be updated to read the CLA HE Licence.
1.3	Policies and procedures are communicated to employees responsible for the administration of the Licence	<ul style="list-style-type: none"> • LSBU has a good training structure. Introductory sessions are offered to all new academic staff on a 1-2-1 basis, and the key conditions of the licence are covered here. More general staff development sessions are offered throughout the year. 	<ul style="list-style-type: none"> • The auditor supports the pending move to make sessions for new academic staff mandatory.
1.4	Copyright policy includes a provision to handle infringement or breach of licence	<ul style="list-style-type: none"> • The severity of infringement is referenced in the copyright policy 	<ul style="list-style-type: none"> • While academics cannot upload to the reading lists, they can to VLE areas and so it is recommended that spot checks be conducted on VLE areas to detect infringements.
1.5	System in place to ensure ownership or legal access or the acquisition of a copyright cleared copy	<ul style="list-style-type: none"> • The TADC system is linked to the library catalogue and so automatically checks ownership 	<ul style="list-style-type: none"> • Depending on the review of documentation in light of 1.2 above, links to the library catalogue might be included in documentation to facilitate the check on ownership
1.6	System in place to ensure the extent limits are observed (e.g. one chapter/ 10%/ one poem/ one article/ etc.)	<ul style="list-style-type: none"> • The TADC system automatically checks extent limits 	<ul style="list-style-type: none"> • No actions
1.7	System in place to ensure Excluded Categories and Works are observed	<ul style="list-style-type: none"> • The TADC system automatically checks repertoire 	<ul style="list-style-type: none"> • No actions
1.8	System in place to ensure international	<ul style="list-style-type: none"> • The TADC system automatically checks repertoire 	<ul style="list-style-type: none"> • No actions

mandate territories are observed		
----------------------------------	--	--

2) Photocopying Policies and Procedures

The Print Room accepts jobs from a range of university staff. When submitting a request, the requester must complete an order form, which includes a statement that the material has been checked in terms of copyright. Further to this, the team is versed in what is considered infringing material and so can spot and raise concerns as appropriate. On the whole however the print room processes original and bespoke material such as module guides, rather than third party published material.

The university also has copiers across the site, and academic staff can conduct photocopying on any one of these on an individual and ad hoc basis. Copiers seen on the day had up to date Notices for Display adjacent to them to remind staff of the key conditions of the licence. These are updated by Estates or Student Services as appropriate.

3) Scanning and Digital Copying Policies and Procedures

At the heart of the institution's scanning system is the Talis Aspire reading list, which sits in the VLE. Reading lists are completed by the vast majority of academic staff, and requests for scanning come via that means. The requests are then collated in the TADC system and automated checks on ownership, extent limits and repertoire conducted. The scanning team then pick up the request, checking details where appropriate if the Talis system has referred the request, and then make the scan from the original source material. If the institution does not own the original a CFP is purchased. The subsequent scan is uploaded to TADC and is then accessible to students. A back-up copy is kept in a secure drive, accessible only to the scanning team.

Digital Copying

The majority of requests to the team are scanning from print, though the Talis system has been set up to accept a copy from an e-resource if LSBU subscribe to it. It was discussed that an institution can decide when to copy from print over digital, except in the case of works mandated via CCC (CLA's agreement with CCC is such that a commercially available digital version must be used over scanning from print; this does not apply to works from global mandating American publishers).

Disembedded images - those not suitably anchored back to their original source - were discussed. These are not processed centrally and it was felt that images would be used at the discretion of the individual academic. Online image searches are referenced in training.

Maintenance of the Course Collection

Formerly, academics were emailed to determine which scans were required for the following year, but, owing to little engagement, the whole collection is rolled over and then work is conducted to identify which modules are not running. It was discussed that the TADC system appears to prevent items excluded in that academic year from rolling over, but, as discussed, it is advised that this is confirmed with Talis.

Further weeding - the removal of scans no longer needed - is at the discretion of the academic or faculty but staff are encouraged to keep their reading lists up to date from a student use perspective.

Reporting

TADC automates reporting, producing the report for submission to CLA.

4) Textbook Substitution

Textbook substitution (TBS), where the licence is relied on to such an extent that it substitutes for primary purchase, was discussed. Reviewing the sample reading lists selected for the audit, TBS is

not considered to be a problem. All lists recommended core reading and directed students to a good number of original texts, with scans being offered as a complement.

5) Virtual Learning Environment (VLE) and Access to the Course Collection

Students gain access to the VLE via authenticated passwords. Authentication is linked to the student record system and so any student leaving the institution will lose access. Students can only see the courses for which they are enrolled. It was noted that the latest iteration of the licence permits students to retain access to copies throughout their degree programme, so it may be that LSBU wish to extend the life of scans so that students can see the material they studied in previous years.

6) Records Check

A random selection of Digital Copies scanned from print from the HEI's 2015-2016 digital copy record form was reviewed to look at the following criteria:

- Inclusion in the CLA repertoire
- Ownership
- Copyright Notice presence
- Quality
- Extent limits observed
- Reported correctly to CLA

Repertoire

One issue arose because at the time the scan was made, the ISBN - 9780465002122 - was excluded. It's since transpired that the ISBN is covered by the CLA Licence, but it is nevertheless worth investigating how the then exclusion made it through TADC.

Ownership

In all cases the original source material was owned by the institution.

Copyright Notice

TADC automatically generates the Copyright Notice, and so all scans were appropriately prefaced with the notice.

Quality

All scans seen in the records check were of a good to excellent quality.

Extent limits

In all but one case, the extent limits were observed – where extracts were over 5% (as was then the extent limit) they were seen to be one chapter or article.

For one course, two extracts from the same material had been copied, exceeding both 5% (and indeed 10%) and also one chapter. The ISBN in question was 9780582282179, on the course LAW_7_CVJ. This should be looked at in the immediate future to see if the problem persists into this year's reading list, and if so, remedied by the removal of one scan. It will also be worth discussion with Talis to see how this occurred.

Reported

In all cases the extracts were accurately reported.

On looking at the wider VLE, there were generally few issues to be found. VLE areas tallied with the conversation of the morning – that academics make third-party material available via the reading lists, using the VLE area to host lecture notes and links to useful resources. That said, there were incidences of disembedded images across subjects, and it is advised that this issue be more explicitly referenced in training in terms of good copyright and pedagogic practice.

One course - DSS_6_PAP – did raise concerns where copies of chapters were made available in the VLE area. These were without a suitable copyright notice to indicate permissions, were of a dubious

quality, and, operating outside TADC, were likely to go unreported. It is advised that this course area be looked at as a matter of urgency and remedial training be conducted.

Conclusion

Overall the compliance of London South Bank University is Good with many Excellent elements. The team has worked hard to push the reading list system with academics, resulting in high levels of engagement. While this in itself is not a matter for licence compliance, it has led to compliant copies of a high quality and a high level of accurate reporting. In order to enhance the grade to a solid excellent, consideration is needed of the wider VLE area and the materials made available there.

Grading Rubric

Excellent	<ul style="list-style-type: none"> No concerns found Excellent policies and procedures in place to ensure compliance with the Licence Licence is fully understood by staff No follow up actions
Good	<ul style="list-style-type: none"> Minor concerns found Good understanding of the Licence Acceptable policies and procedures in place to ensure compliance with the Licence Recommendations made to improve areas of weakness
Satisfactory	<ul style="list-style-type: none"> Some concerns found Adequate understanding of the Licence Basic policies and procedures in place to ensure compliance with the Licence Recommendations made to improve areas of weakness
Unsatisfactory	<ul style="list-style-type: none"> Concerns found in understanding of Licence and/or adherence to the Licence Weak and/or lack of formal policies and procedures in place to ensure compliance with the Licence Recommendations made to improve understanding and improve areas of weakness Training strongly recommended Action Plan recommended

Overall Assessment

Overall compliance with Higher Education Licence	Good
Adequacy of documentation of internal policies and procedures	Good/Excellent
Understanding of copyright and the Higher Education CLA Licence	Excellent
Records check	Excellent
Virtual Learning Environment and access to the course collection	Good

Good Practice, Recommendations and Actions

Good Practice

- The training and advice offered to staff is excellent. The documentation is clear and appropriate for the audience, sitting the CLA licence in the context of the wider landscape of copyright. The training sessions given to new staff, and those as a drip-feed to existing staff are also evidence of good practice.

2. The records check was very strong. The use of Talis to automate checks and the use of high-quality scanners has led to an excellent level of scan. The structure of the reading lists is such that there is little concern regarding textbook substitution.
3. The security of the copies made is excellent.

The Auditor recommends that the actions and recommendations identified are completed within 12 months

Recommendations

1. The institution has made great strides in terms of scanning in the context of the reading list software, but should now consider how to ensure compliance outside of this environment.

Actions

1. It should be clarified with Talis what happens to newly-excluded items. Are they rejected at rollover or is manual intervention needed?
2. Disembedded images, and how to treat the them, should be explicitly addressed in training and guidance.
3. Our look at the wider VLE suggests that spot checks are required to monitor staff activity. Where appropriate remedial training can be implemented.

© The Copyright Licensing Agency Ltd 2017

[The Copyright Licensing Agency Ltd](#)

Barnard's Inn, 86 Fetter Lane, London, EC4A 1EN

Tel 020 7400 3100 Fax 020 7400 3101 Email cla@cla.co.uk www.cla.co.uk

Registered in England. Reg no. 1690026

	CONFIDENTIAL
Paper title:	Anti-fraud, bribery and corruption report
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Natalie Ferer, Financial Controller
Executive/Operations sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	To alert the Committee to any instances of fraud, bribery or corruption arising
Recommendation:	The Committee is requested to note this report

Summary

Since the last report there are no new incidents to report.

The Committee was made aware at the last meeting of an incident where four requests to change employee bank accounts were received and actioned by a member of the Payroll team.

In line with the University's Fraud Response plan, the police were informed via the Action Fraud online reporting site. Action Fraud do not routinely feedback the outcome of reports and we are not expecting the police to take specific action in relation to our report. PwC were brought in to review the matter and their letter containing their findings is attached with recommendations for further action listed from page 6 of their report.

Audit Committee should note PwC's comment on reporting the fraud. Executive did not deem it to be significant and therefore did not report the matter to HEFCE. A "significant" fraud is one where the amounts are significant, where officers of the University are involved, where the particulars are novel or contentious, or where there is likely to be public interest. Executive considered that the scale and fact that this appeared to be a phishing attack did not meet this criteria. Executive remains of this view.

Recommendation

The Committee is requested to note this report.

This page is intentionally left blank



Private and confidential

Richard Flatman
Chief Financial Officer
London South Bank University
103 Borough Rd
London
SE1 0AA

CC: Natalie Ferrer

12 January 2018

Dear Richard

INCIDENT RESPONSE SUPPORT

1) Background

During September 2017, the London South Bank University (“the University”) experienced an incident whereby a series of invalid changes to employee bank details were processed on the University’s payroll system. This resulted in the monthly salaries of at least three employees (with a fourth suspected case still under investigation) being diverted into another bank account with a total potential loss to the University of £14,947.94. An initial investigation performed by the University’s Head of Information Security identified that the University email accounts of at least three employees had been compromised, allowing a fraudulent bank detail amendment request to be sent to the Payroll Team for processing from each of the three email accounts. In response, changes to payroll bank detail amendment processes have been made, and the incident has been reported to Action Fraud by the University.

You asked us to provide specialist advice to the University following the incident response to comment on the investigation carried out and make observations on any potential:

- additional investigation procedures that could be performed and lines of enquiry that could be pursued; and
- further measures that could be considered to prevent an incident re-occurrence.

Our scope, approach and summary of observations are set out below.

2) Scope and approach

In order to review the University’s response to the incident, a Cyber Specialist and Corporate Investigations Specialist conducted a site visit with the objective of obtaining an understanding of:

- What is known about how the incident was perpetrated;
- The steps taken to investigate;
- The evidence collected; and
- The steps have been taken to prevent further incidents from occurring.



This was achieved through:

- Conducting exploratory meetings with
 - The Head of Information Security
 - The Financial Controller
 - The (new) Interim Payroll Manager
- Reviewing available investigation outputs, supporting documentation and evidence in relation to the internal investigation

3) Limitations

Our work was limited to the scope and approach set out in our terms of reference. Our review did not involve:

- Performing any investigative procedures; or
- Performing any controls assessments

4) Summary of incident response

The incident was first detected when an employee (Person A) informed the University's Payroll team that they had not received their September 2017 monthly salary. As amendments had been made to the employee's payroll bank details during the previous month, the Payroll Manager suspected an irregularity and informed the Financial Controller. The Financial Controller invoked the University's fraud response plan and commenced an investigation with technical support from the Head of Information Security.

The findings from the investigation suggested that Person A's University email account had been compromised by an unknown person(s), potentially through the Outlook Web Access system (which allows users to access their University email account from non-University owned equipment.). This had enabled a fraudulent bank detail amendment request to be sent to the Payroll team for processing from Person A's email address. A review of all amendments to employee bank details processed by Payroll during September 2017 identified a further three bank detail amendments. Payroll has sought to contact the three employees, and have confirmed that two of the amendments were fraudulent as the salaries were not received by the employees. At the time of our site visit, Payroll were still trying to make contact with the third individual.

We were informed during our meetings with the three stakeholders listed above that the following steps have since been taken by the University following the initial investigation in response to the incident:

- The four employees affected have been required to change their system passwords;
- A password change has been forced across the university for all employees in order to expose any remaining compromised accounts;
- All University machines used by the known victims have been scanned using anti-virus software in order to reduce the possibility of a malicious software presence on them that compromised the victim's credentials, or that may have been unintentionally introduced by the users after compromise;



- Advice has been provided to three of the four confirmed affected employees on ID fraud due to a risk that some of their personal details are now available to other criminals; and
- An additional control has been added to the employee bank details amendments process, whereby requestors are required to provide in person a completed change of details request form and evidence of identification to the Payroll team

The matter has been reported to the police by the Financial Controller through the Action Fraud website. However, no report has been made to Higher Education Funding Council for England (“HEFCE”), as the University have calculated the potential loss to be under the reporting threshold of £25,000.

5) Cyber aspects

The landscape

Staff and employees of the University have Microsoft Office365 accounts. Users identify and authenticate themselves to the system using single factor username and password. As well as accessing their accounts from University-owned end points, they are also able to use their Office365 account through browsers on their own equipment and mobile devices. The Staff and Employee Office365 accounts are hosted on-premises (although these are moving to the cloud in future).

Some staff and employees have University issued laptops, but the majority use shared desktop machines on University premises, or log in from their own devices.

The same credentials are used to identify and authenticate the user on Active Directory for other University systems (Single Sign On –SSO). For example, the HR system that holds personal information about the user, the University Intranet and Staff Directory.

The Head of Information Security states that the University has a quarterly patch cycle across all managed systems, a process for carrying out urgent security patches and an Incident Response process in place. There are some obsolete systems (for example that running CCTV), but these were not a factor in this incident.

The Head of Information Security was aware of at least one similar attack in another Higher Education establishment.

The cyber investigation and limitations

The initial cyber part of the investigation looked for any evidence that Person A’s Microsoft Office365 credentials had been compromised. Through examining logs, the Head of Information Security was able to identify that suspect emails were sent through Outlook Web Access (OWA), which is the access mechanism that allows users to work from non-University owned equipment. The Head of Information Security then tried to identify the source IP address(es) of the suspect sessions, but found a previously unknown forensic limitation – they were unable to resolve the source IP addresses at the incoming connection load balancers, and were therefore unable to determine where the suspect sessions originated.



The Head of Information Security checked for Person A's username on a publicly available list of known compromised account and found that those credentials were listed. This meant that it was likely that the attack involved compromised credentials.

All University owned machines used by the compromised user accounts have been checked for viruses and malware. The University has no means of checking the users' personal machines or devices for malicious software.

Likely compromise method

The Head of Information Security held the view that the most likely compromise method used was a successful phishing attack. In common with many organisations, the University is frequently subject to these. Based on our experience of dealing with compromised credentials, we concur that this is the most likely compromise method, but we have not seen any evidence that this was the method used. It is not however the only possible method (as set out below).

Additional considerations arising from the credential compromise

What else could an attacker have done?

Compromise of these credentials can enable an attacker to take several malicious actions. These could include:

- Harvesting additional personal information about the compromised users, for example from the HR system. There is some evidence that this occurred because their personal addresses were used on the amendment forms (although at the date of our fieldwork, these addresses had not been verified - see Potential Further Investigation Procedures).
- The attackers could have changed personal details held by the University, for example phone number or address in order to compromise any multi-channel controls (such as a verification phone call).
- As well as the fraudulent emails amending bank account details, compromised accounts are also commonly used in further phishing attempts as the emails come from a 'trusted' person.
- The credentials could have provided a foothold inside the University systems for more advanced attacks to take place.
- The attackers had access to the users' diaries. The investigation noted that the fraudulent emails were all sent at points where the users were conveniently not around (on leave) to spot the malicious activity. There are several ways this could have been achieved, but the simplest would be for the attacker to log in, but take no action other than checking the users' diaries to look for a good time to commit the fraud.

We were advised that sensitive information about students was not accessible from the compromised accounts, unless they are included in emails to/from the impacted accounts.

None of the staff impacted had access to any sensitive systems, or elevated privileges.

What checks have been carried out for other exploits using the compromised credentials?



The Head of Information Security has examined logs of all activity for the compromised accounts, but did not identify any suspicious activity.

What if credentials were compromised using a different method to phishing?

If the credentials were compromised by a technique other than phishing, it is possible that the attack could still be underway, and changing passwords will not prevent further malicious activity. Different methods have different implications:

- Shoulder surfing¹ – Password change would resolve the breach. Training would be required to prevent re-occurrence.
- Keylogger² on users' personal machine – New credentials following a password change would be harvested.
- Keylogger on University owned machine – New credentials following a password change will be harvested. Checks have been carried out on all machines used by the compromised accounts to sweep for malicious software, including software keyloggers.
- Hardware keylogger on University owned machine – New credentials following a password change will be harvested. This compromise would not show up on a scan of the machine. Although this attack involves risk of detection, and requires physical access to the machines, the fact that 3 of the 4 potentially compromised users work in the same building (on 2 adjacent floors) means that the risk should be considered. One possible control is a physical inspection of the machine and peripherals should compromise re-occur.
- Attack on Active Directory – Although this is a possibility, it is unlikely because of the effort involved. Redirection fraud on payroll tends to work on a single occasion as staff would be likely to report a missing salary payment. The potential gains from this method would not make investment in an advanced compromise likely. Active Directory has logging and monitoring in place to detect and investigate unauthorised changes.

Could other accounts have been compromised?

There is a risk that there are other, undetected, compromised accounts in the pool of staff and employees. Therefore, the Head of Information Security is discussing a 'national password change' day where all staff and employees will simultaneously be forced to change their passwords. This is a means of flushing out any remaining compromised accounts. If the legitimate user changes the password, the attacker's credentials are rendered useless, but if the attacker changes the password, the user will be unable to log in and will contact IT who will disable the account immediately.

The Head of Information Security has considered how to carry out 'watching' analysis of all accounts, but this is problematic because of the infrastructure limitations.

Registering the University domain for notifications from a 'publicly owned' list may help to expose other compromised accounts.

¹ "Shoulder surfing" is the practice of observing somebody entering credentials. For example, standing close enough to watch a user enter a password at a computer or PIN number at an ATM.

² The term "keylogger" refers to an attack used to obtain sensitive information by recording all keystrokes made on a system. Used to identify and capture passwords. This is commonly a covert piece of malicious software installed on a poorly protected system, but the attack can also be carried out using a specialist piece of hardware inserted between the keyboard and casing of a desktop PC, or using a compromised keyboard, thus making it impossible to detect using malware detection.

6) Suggested further investigation procedures

Based on our understanding of the investigation procedures performed to date, we have identified the following additional investigative procedures for consideration:

- An electronic search of all employee, supplier and student standing data held on University systems to detect whether any of the bank account numbers to where the monies were diverted are present. This would help to identify any potential links to employees, suppliers or students, or identify any further potentially fraudulent transactions or requests.
- A search of all University email traffic using the bank account numbers to where the monies were diverted as search terms. This would help to identify any potential links to employees, suppliers or students, or identify any further potentially fraudulent transactions or requests.
- It is understood that one potential victim has not made contact with payroll to report a missing salary, and has also not responded to contact from payroll. The lack of contact should be escalated to the employee's line manager to confirm that they are still performing their contracted duties and working hours.
- Change of address/bank detail forms appear to have been completed by the fraudster(s) on behalf of the four victims. These should be followed up with Human Resources to confirm whether the addresses are those of the victims, or whether address details had also been amended on HR systems, which would could present an additional risk of mail redirection.
- Checks of machines used by the compromised accounts for malicious physical devices (see keyloggers above).
- Checks of the other compromised University accounts on public 'owned' lists of stolen credentials.
- Registering the University domain for notifications from a public "pwned"³ list may help to expose other compromised accounts.

In addition, there is an inherent risk that the fraud could be linked to wider organised criminal, or even terrorist, activity. The University should report the matter to the relevant banks so that their internal counter fraud and anti-money laundering teams are able to investigate further. Furthermore, as noted above, the matter has not been reported to HEFCE as the University have calculated the potential loss to be under the reporting threshold of £25,000. However, we note that HEFCE may consider incidents to be serious enough to warrant reporting even if the loss is under £25,000 if the incident meets certain criteria, including being "novel, unusual or complex". Whilst this is criteria is highly subjective, the nature of the incident could be construed as such. Reporting the incident would allow HEFCE to warn other institutions, which could help them to avoid becoming victims.

7) Suggested further remedial measures

As set out above, the university has taken a number of measures following the incident to seek to minimise the risk of repeat incidents. We have identified the following further measures that could be considered:

- The changes to the bank details were all processed by one individual, the Interim Payroll Manager. Whilst it is understood that the defined process was followed and controls were

³ "Pwned" is originally a slang term that has entered common usage in the information security community. In this context, it means 'compromised credentials', hence 'pwned list' is a list of known compromised credentials or domains.

complied with, we note that some potential warning signs of fraud did not appear to have spotted (listed below). As bank mandate fraud appears to be on the increase nationally and fraud schemes becoming more sophisticated in nature, staff who are responsible for processing amendments to supplier and employee bank detail could perhaps benefit from fraud awareness training. The potential warning signs missed in this case were:

- Invalid signature: The signature on the request form relating to one of the victims (Person A) would not have matched specimen signatures held by Finance (though it is noted that procedures did not include checking against specimens, particularly as specimens do not exist for all staff).
- Multiple bank accounts: The first change of bank details request relating to Person A was not correctly processed by the Interim Payroll Manager, resulting in the change of details failing. A second request for an amendment form was then submitted, using a different bank account at a different bank. Despite the attempts being made close together, and the unusual behaviour of changing banks rather than re-confirming the first set of bank details and the signatures on the form being completely different, the second attempt was successfully processed by Payroll.
- Urgent funds request: Once the amendment was actioned, emails were then sent from Person A's email account to Payroll referring to a need for "urgent funds due to a serious family medical condition" and requesting access to the employee's pension fund.
- Handwriting patterns: The change of details request form completed for the four individuals appeared to contain similar handwriting.
- Unusual pattern: The four potentially fraudulent amendment requests represented a spike in activity. It is understood that the typical volume of requests during the year was one per month, whereas four requests were received in the space of a month
- Payroll had previously introduced a control into the amendment process whereby staff are required to complete and sign a change of details form. However, Payroll do not check signatures against specimens, and so it is unclear as to how the form would provide any additional safeguards against fraud. Since the incident, Payroll have introduced a new control whereby employees are required to visit the payroll section in person to provide the completed form along with ID. Whilst this is a robust control, it may prove difficult to implement where staff are not based in London. A call back option to verify requests could be considered using contact numbers held on University systems (although given that the attackers were able to access and change personal details using their hijacked credentials, this control could also have been subverted in this case).
- Multi-factor authentication on Microsoft Office365 user accounts will reduce the probability of compromised credentials being exploited. The Head of Information Security is discussing this additional control with the Board.
- Putting a user's personal information, and the ability to change personal information on University systems, behind an additional layer of access control – for example a PIN or additional password on the HR system not linked to SSO. This would prevent a malicious user who has compromised the Microsoft Office365 credentials from accessing or changing highly sensitive data, and would prevent them from compromising a second authentication channel (for example a phone number or SMS). This is an example of a layered defence.
- Improving Cyber Forensic Readiness: The incident exposed some limitations in the forensic readiness of the University's systems. A coherent Forensic Readiness assessment and remediation plan, followed by testing, will improve the University's ability to respond to future attacks.



- Improving users' cyber knowledge: Although all staff and employees are given awareness training, like many organisations, people are often the weakest link. This is exacerbated when users are able to use their own devices, which may not have basic security measures in place. Improving knowledge and the traction of the training may help to improve the University's overall security posture.
- Registering the university domain on a public 'owned' list in order to receive notifications of any usernames that have been, or will be, published as compromised. This action is in progress, but requires that you provide evidence that you are the owner of the DNS record of the organisation (which is currently being addressed by the Head of Information Security).
- The University could consider taking a feed of Threat Intelligence to identify when they are being targeted and by whom.

Yours sincerely,

Justin Martin - Partner
PricewaterhouseCoopers



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 16 October 2017. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

This is a draft prepared for discussion purposes only and should not be relied upon; the contents are subject to amendment or withdrawal and our final conclusions and findings will be set out in our final deliverable.

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.

© 2018 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:	Speak up report
Board/Committee:	Audit Committee
Date of meeting:	8 February 2018
Author:	Joe Kelly, Governance Officer
Sponsor:	James Stevenson, University Secretary
Purpose:	To note
Recommendation:	The committee is requested to note the report.

Executive Summary

Outstanding case: SBUEL employment

Following the speak up case raised on 17 July 2017, regarding unfairness between LSBU and SBUEL terms and conditions (previously reported to the Audit Committee on 3 October 2017), the Pro Vice Chancellor (Research and External Engagement) and the Executive Director of Organisational Development and HR have reviewed the staffing aspects of SBUEL. Their report was discussed by the University Executive on 22 January 2018 and is currently being reviewed by the Chair of the Audit Committee.

Other cases

There are no new cases reported since the last meeting of the Audit Committee on 9 November 2018.

This page is intentionally left blank

CONFIDENTIAL	
Paper title:	Data Assurance Report
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Richard Duke – Head of Planning, Performance & Assurance
Executive/Operations sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	For Information; to provide Committee with a report on data quality risk assessment.
Which aspect of the Corporate Strategy will this help to deliver?	Effective management of data quality relates to the entire organisation, but relates particularly to goals 7 (People & Organisation) and 8 (Resources & Infrastructure).
Recommendation:	Committee is requested to note: <ul style="list-style-type: none"> • the report

Executive Summary

The Data Assurance Group report identified some risk areas in relation to core systems, especially regarding data flow between systems, which could pose risks relating to data quality and thus decision making.

An institutional approach is considered the optimum solution to addressing these issues, rather than a piecemeal system basis. The work currently relating to the GDPR compliance project, which was approved by the Executive in January, and LEAP, the Student Journey Transformation Project, will enable greater definition of data architecture and help address the issues currently identified (overview on page 3).

- The Committee is requested to note the report

This page is intentionally left blank

Data Quality – Data Assurance Group (DAG)

Executive Summary

Since 2014, LSBU has been undertaking data audits of its core systems. As a result of this process, considerable progress has been made against a number of controls across all systems. Despite this however, the overall Data Quality Risk Level remained at high or very high for core systems. The previous Data Assurance Group report summarised weaknesses as follows:

In summary, LSBU has room for improvement in relation to the following control areas:

- Procedures relating to how data is input into systems
- Knowledge of what data is held in systems and how this data feeds other systems
- Access to systems and processes around the sharing of data

The risks to LSBU as a consequence of these System Risk Ratings

- Poor decision making, and therefore loss of competitive advantage
 - Slow and reactive decision making
 - Poor decisions as based upon inaccurate data
 - Lack of trust in data by decision making reducing ability to make evidence informed decisions
- Unable to build a culture of accountability
- Inaccurate external returns (funding/reputation consequences)
- Inability to automate processes resulting in reduced efficiency
- Data protection/security risks
- Litigation risks relating to data protection and CMA
- Unable to deliver a CRM system

Response

The challenges identified in relation to levels of data control, need to be solved through institutional led initiatives, rather than system by system. It was decided therefore, that further system data audits should be postponed, until work was undertaken through the General Data Protection Regulation (GDPR) project. Until detailed data audits and data flows have been identified and documented, improvements at institutional level will be difficult to achieve. The GDPR project is the perfect avenue to address these issues.

Also, the Student Journey Transformation Project (LEAP) will also allow the institution to define data flows and its architecture, allowing for significant improvements in data flow process and data documentation.

The controls as part of the system data quality assessment exercise that will be addressed through GDPR and LEAP are:

Control #	Area	Control
3	Accountability	There is a clear audit trail to changes to data which can be tracked by user making changes, and it is clear whom each user's line manager is.
4	Governance	The technology for storing data is demonstrably understood.
5	Governance	The technology for data sharing is in place and demonstrably understood.
6	Governance	Arrangements are in place for carrying out systems testing after changes to the system. This will include user acceptance testing.
7	Governance	Security arrangements for all information systems are in place and are monitored regularly.
16	Understanding Data	All data items, in a single document are defined, with clear definitions, source, input method, role accountability, data standards (including mandatory fields), archiving requirements, rapid recovery requirements and who it can be shared with.
17	Understanding Data	LSBU data dictionary is referenced in all outputs (where appropriate)
18	Understanding Data	The ability to triangulate data from other systems is reviewed and documented on an annual basis, with updates made where inconsistent formats found
19	Understanding Data	Data Standards are reviewed annually, with requirements for mandatory fields or consistent input rules defined (using Data Item doc).
20	Reporting	Where there is joint working with external partners, there is an agreement covering data quality with partners (for example, in the form of a data sharing protocol, statement, or service level agreement).
21	Reporting	All reports should reference whether they adhere to the data quality "Gold Standard".

Recommendations

- System data quality control audits resume in the summer of 2018, after the completion of the initial GDPR project.
- The DAG meets in September 2018 to review progress.

PPA – January 23rd 2018

Appendix A - Systems Data Quality Checklist Summary as of December 2017

System Reviewed	Payroll (i-trent)	Registry (QLS)	SALTO/Card Exchange	Raiser's Edge	Finance (Agresso)	OSHENS	CMIS	HR (Oracle)
Current Data Quality Risk Level	High	High	High	Very High	High	Very High	Very High	Medium
Current Data Quality Risk Level - Excluding Institutional Led Controls	Low	Medium	Medium	Medium	Medium	High	High	
Previous Risk Level	High	High	High	High	Medium			
Dec 2016 Review Score - Excluding Institutional Led Controls		78%	84%	72%	88%	63%	56%	
Dec 2016 Review Score		54%	53%	45%	59%	42%	35%	
July 2016 Review Score (different checklist methodology)	64%	64%	51%	56%	-			-
December 2015 Review Score	79%	75%	-	-	80%			83%
October 2015 Review Score	79%	75%	-	-	81%			74%
Data Trustee	Richard Flatman	Ralph Sanders	Carol Rose	Gurpreet Jaggpal	Richard Flatman	Mandy Eddolls	Carol Rose	Mandy Eddolls
Data Steward	Natalie Ferer	Ralph Sanders	Carol Rose	Mike Simmons	Natalie Ferer	Ed Spacey	Carol Rose	Joanne Monk
Data Manager	Denise Sullivan	Lisa Upton	Elizabeth Palicza	Olivia Rainford / Ian White	Ravi Mistry	Sam-Kee Cheng	Ronnie Chandler	Dave Lee

Control #	Area	Control	Data Quality Control Assessment						
1	Accountability	The Data Steward has overall strategic responsibility for data quality, and this responsibility is not delegated.	In Place	In Place	In Place	In Place	In Place	In Place	In Place
2	Accountability	The system requires logins which cannot be shared.	In Place	In Place	Partially in Place	In Place	In Place	In Place	In Place
3	Accountability	There is a clear audit trail to changes to data which can be tracked by user making changes, and it is clear whom each user's line manager is.	Partially in Place	Absent	Absent	Absent	Absent	Absent	Absent
4	Governance	The technology for storing data is demonstrably understood.	In Place	Absent	Absent	Absent	Absent	Absent	Absent
5	Governance	The technology for data sharing is in place and demonstrably understood.	Absent	Absent	Absent	Absent	Absent	Absent	Absent
6	Governance	Arrangements are in place for carrying out systems testing after changes to the system. This will include user acceptance testing.	Absent	Absent	Absent	Absent	Absent	Absent	Absent
7	Governance	Security arrangements for all information systems are in place and are monitored regularly.	Absent	Absent	Absent	Absent	Absent	Absent	Absent
8	Governance	A business continuity plan is in place to provide protection for records and data which are vital to the continued functioning of the service.	In Place	Partially in Place	In Place	Partially in Place	In Place	In Place	Absent
9	Governance	Policies and procedures relating to data collection, sharing, storage and reporting are held and should be reviewed annually.	In Place	Partially in Place	In Place	Partially in Place	Absent	Partially in Place	Partially in Place
10	Governance	Systems identified as high risk or very high risk are included as risks in the local risk register and actions as part of the LDP process.	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
11	Governance	All staff with access to the system, must have undertaken data protection training.	In Place	In Place	In Place	In Place	In Place	In Place	In Place
12	Governance	There is a framework in place to review data quality, which has been approved by the accountable data steward. Review outcomes are reported to the DAG and followed up, with corrective action taken.	Partially in Place	In Place	Partially in Place	Partially in Place	Not Applicable	Not Applicable	Not Applicable
13	Governance	All external returns follow LSBU data governance sign off policy.	Absent	Partially in Place	Not Applicable	Not Applicable	In Place	Absent	In Place
14	Staff Skills	Job descriptions reflect the requirement for postholders to adhere to data quality and generate data that is accurate, valid, reliable, timely, relevant and complete. Where this does not occur from a postholder, mitigating strategies are reviewed.	In Place	In Place	In Place	In Place	Partially in Place	Partially in Place	Absent
15	Staff Skills	Staff receive regular training in relation to data quality and have access to all relevant operational policies and procedures (ideally using information systems).	Partially in Place	Absent	Partially in Place	Partially in Place	In Place	Absent	Partially in Place
16	Understanding Data	All data items, in a single document are defined, with clear definitions, source, input method, role accountability, data standards (including mandatory fields), archiving requirements, rapid recovery requirements and who it can be shared with.	Partially in Place	Absent	Absent	Absent	Absent	Absent	Absent
17	Understanding Data	LSBU data dictionary is referenced in all outputs (where appropriate)	Not required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
18	Understanding Data	The ability to triangulate data from other systems is reviewed and documented on an annual basis, with updates made where inconsistent formats found	Not required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
19	Understanding Data	Data Standards are reviewed annually, with requirements for mandatory fields or consistent input rules defined (using Data Item doc).	Not required	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
20	Reporting	Where there is joint working with external partners, there is an agreement covering data quality with partners (for example, in the form of a data sharing protocol, statement, or service level agreement).	Absent	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
21	Reporting	All reports should reference whether they adhere to the data quality "Gold Standard".	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
22	Reporting	Same base data is used for internal and external reporting	In Place	In Place	Not Applicable	Not Applicable	In Place	In Place	Not Applicable
23	Reporting	External definitions are applied in all internal reporting, where available and appropriate, in supporting one version of the truth principle	Not Applicable	Partially in Place	Not Applicable	Not Applicable	In Place	Absent	Not Applicable
24	Reporting	Data should not be shared without an understanding of how data will be used and kept in the loop as to how used and reports fed back (e.g. cc'd in an email when distributed)	Absent	In Place	Absent	Absent	In Place	Absent	Absent
25	Reporting	All outputs are checked and referenced to an expected outcome by appropriate staff (if deemed as required), to support accurate reporting of data.	In Place	Absent	In Place	Absent	Partially in Place	In Place	Absent

This page is intentionally left blank

Paper title:	General Data Protection Regulation compliance project update
Board/Committee	Audit committee
Date of meeting:	8 February 2018
Author:	James Stevenson, University Secretary
Purpose:	To note
Recommendation:	The Committee is requested to note the update.

Executive Summary

The first meeting of the GDPR compliance project board was held on 17th January 2018. The project board discussed the project plan and agreed the operational leads in each key area of the university.

In addition, the project board considered the following:

1. the key recommendations from the PwC “special characteristics” report (attached), which include:
 - formulate the GDPR vision and strategy (this will emerge as the project takes shape);
 - appoint a data protection officer. A new, more senior DPO role has been established (replacing the vacant information compliance role). The DPO role has been offered to a candidate, currently awaiting confirmation;
 - carry out a data mapping exercise (see below);
 - map GDPR requirements for each area to establish which GDPR principles should apply;
 - adopt a risk-based approach to prioritising which areas to address;
 - conduct a gap analysis of LSBU’s data protection / GDPR paperwork (see below);
 - conduct a technology functionality gap analysis;
 - “methodise the new privacy big pillars”. The “pillars” are: accountability, policy, privacy by design, records of processing, breach notification, impact assessments, data protection officer (the compliance project will address each of these pillars);

- “stress test” LSBU’s data protection framework to see how it will withstand adverse scrutiny (appropriate testing will be built-in to the project plan).
2. The key phase taking place now is mapping flows of personal data. The project manager is liaising with managers of the key data systems to build the maps (taking account of the pressures of day to day activity in some student-facing teams).
 3. The next step is to review and agree the “legal basis for processing” for each data flow.
 4. The priority policy documents have been commissioned from external lawyers.
 5. In collaboration with a number of other HEIs, standard third party terms & conditions of processing have been commissioned and will shortly be agreed.

The next meeting of project board will be held in late February 2018 (and continuing monthly).

An update will be reported to the next meeting of the audit committee.

London South Bank University

Draft - GDPR Special Characteristics and Road Map

*Draft for discussion
December 2017*

Contents

<i>Executive Summary</i>	2
<i>Background</i>	2
<i>Approach</i>	2
<i>What is data protection?</i>	2
<i>GDPR in the context of LSBU</i>	2
<i>Setting a vision for your GDPR programme</i>	3
<i>The risk-based approach and the ‘Work-Time Paradox’</i>	3
<i>High level recommendations</i>	4
<i>Special Characteristics Workshop</i>	10
<i>Themes</i>	10
<i>What does ‘data privacy’ mean to LSBU?</i>	11
<i>What does ‘risk’ mean to LSBU?</i>	13
<i>What does “good” look like to LSBU?</i>	15
<i>Appendix 1: LSBU’s Recommended Roadmap</i>	1
<i>Appendix 2: LSBU’s Readiness Assessment Results</i>	2
<i>Appendix 3: Attendee List – Special Characteristics Workshop</i>	5

Executive Summary

Executive Summary

Background

PricewaterhouseCoopers LLP (“**PwC**”) was instructed by London South Bank University (“**LSBU**”) to undertake a GDPR Readiness Assessment and Special Characteristics Workshop, as part of LSBU’s preparations for the forthcoming European Union (“**EU**”) General Data Protection Regulation (“**GDPR**”). The GDPR, which will take effect from 25 May 2018, imposes radical changes to the current data protection regulatory framework in Europe and contains a series of new rules that will require LSBU to revisit and refresh its data protection practices.

Approach

Following a GDPR Readiness Assessment carried out by PwC of LSBU on the 22nd June 2017, a Special Characteristics Workshop was conducted on 30 November 2017. The Special Characteristic Workshop was a facilitated discussion that provided a high level overview of the GDPR to LSBU and focussed on LSBU’s understanding of the concept of data privacy/protection; what it considers ‘risk’ to mean and its views on what a ‘good’ approach to data privacy/protection looks like. The remainder of the workshop focused on taking through LSBU through a non-prioritised GDPR programme plan. During the workshop we addressed each of the workstreams in the plan and identified what work LSBU has done to date and what activities should have greater priority, including the expectations for LSBU to complete actions in the road map.

What is data protection?

In this report, reference to data protection means the operational and technical measures that are necessary to ensure that personal information is handled properly, safely and legitimately by reference to European standards and expectations. These measures, which are generally seen as necessary components of good organisational behaviour, have helped to shape the legal and regulatory frameworks governing the handling of personal information and vice versa.

Personal information or personal data means information which relates to a living individual. Although there is often debate about the extent to which information (or data) should be considered to be personal, a simple construct to work from is that personal information will usually arise where the behaviours or characteristics of an individual (or the way an individual uses their electronic devices) are recorded or tracked by reference to a name or unique identifier such that an individual could be identified.

The concept that personal information should be handled properly, safely and legitimately includes requirements for data quality (i.e. personal information should be accurate), data retention and data security; requirements concerning the purposes for which personal information can be handled; requirements concerning how personal information can be shared; requirements for transparency about handling; and requirements that help individuals to maintain a degree of control over their personal information. These concepts are contained in many pieces of data protection legislation globally.

GDPR in the context of LSBU

LSBU is a tertiary educational institution mainly located in the UK, but has global reach having multiple partnerships with education institutions globally. Personal data is at the very heart of LSBU as the University holds information relating to millions of student’s. Reasons for retaining the information ranges from legal obligations to day to day business operations and marketing requirements. The personal data held also allows LSBU to maintain student records, oversee and manage their academic progress and conduct research vital to the operations within the University.

LSBU has a desire to achieve a balance in their GDPR compliance to ensure they are not disadvantaged within the educational sector, nor failing their students or partners with poor data protection policies, systems and procedures. LSBU wishes to “do the right thing” with data, but are aware that under the timeframe that full compliance may not be achieved. This was the clear message in both the R.A.T and the Special Characteristics Workshop.

Provided that LSBU takes an efficient approach to data handling, it should be able to thrive in the post-GDPR world. LSBU are encourage to consider the GDPR as an opportunity for doing the right thing for its students, organisational growth, efficiency gain and other positives, such as “an opportunity to mature”, rather than a compliance burden. In the educational system, it will be those organisations with a good, logical and efficient approach that will prosper both within the UK and globally.




Setting a vision for your GDPR programme

In our view, it would be unwise to go beyond the preliminary steps of a GDPR programme without setting a Vision for what LSBU want to achieve. In the absence of a Vision, LSBU may end up undertaking ‘purposeless activities’, which fail to address all the considerations and risks that are relevant. This can be looked at in a number of ways.

First, business transformation programmes need a Vision to provide instruction to all parts of the business and a yardstick for the development of KPI’s and metrics. A Vision will sustain the programme over time, so that it survives the attrition of personnel and the distorting effect of crisis and parochial or transient concerns or interests. A Vision can also help to provide an organisation with a narrative to answer challenges and adverse scrutiny. For example, we anticipate that the Information Commissioner (ICO) will look closely at an organisation’s Vision in serious cases, albeit we accept that this might not necessarily be the language used.

The idea of purposeless activity is worth looking at in the context of regulatory enforcement activity. The trend of case law, here and abroad, which PwC is tracking, is that organisations are coming into conflict with the regulatory system despite their investments in data protection ‘compliance’ work. That tends to suggest that the work that is being done isn’t addressing real risk, or the important risks first. A Vision should help an organisation avoid this trap.

When developing a GDPR approach, it is important to consider the following three key elements:

Business and economic goals 	Effective data processing can act as an asset that drives the organisation. For example, it can be used to develop new services, provide targeted marketing or improve efficiency. So how will your Vision support, or not hinder, the progression of your business and economic goals?
Risk 	Effective risk management involves understanding what risk actually means, your unique risk profile and appetite, and identifying meaningful controls that get the job done. What risks are you concerned about, which will you terminate, treat or transfer and are there any that you will simply tolerate?
Compliance obligations 	The GDPR plainly contains compliance goals, but you need to look at your obligations in the broadest sense and weigh-up their impacts. Do you have contractual positions that are currently immovable? Do your corporate ethics somehow ‘raise the bar’? Have you got obligations that somehow conflict with the GDPR?

In our view, it is important to look at these issues together, in a holistic manner, rather than individually, or in isolation. For example, an overly restrictive view of a technical legal compliance issue might not deliver any meaningful outcomes for operational risk, nor may it be supportive of your economic goals.

The risk-based approach and the ‘Work-Time Paradox’

PwC considers that many organisations will find it impossible to become fully compliant with the GDPR in the 5 months that remain until May 2018. Furthermore, PwC is of the opinion that the legislation is built on a false

assumption about the current data protection maturity levels in most organisations. Therefore, the GDPR is placing a greater transformational burden on organisations than the law has anticipated. As such, a state of continuing unlawfulness is likely even in the best run organisations in May 2018.

We have called this the “Work-Time paradox” as organisations have too much to do and too little time in which to achieve it. This must be factored into any GDPR remediation activity as it will fundamentally alter how LSBU approach their GDPR plans. LSBU will not be able to complete every GDPR compliance activity contained in the GDPR and therefore a risk-based prioritisation of compliance activity is necessary, as the only alternative to a full compliance approach. While the GDPR requires total legal compliance, in reality Articles 24 and 35 (in particular) lead to the view that the GDPR itself requires a risk-based approach.

It is also important to note that data protection is about a lot more than compliance and law; good data handling is a critical business issue in its own right, which has the potential to add considerable value across the whole of the business and in which every part of business needs to be involved. This is why PwC advocates a steering committee or working group that is comprised of a range of stakeholders. By involving key stakeholders from across the organisation, LSBU can avoid the business privacy agenda being driven from a single perspective.

Further, it would be unwise to launch into GDPR preparatory work without having identified a Vision, as this may fail to achieve efficient and effective use of limited time and resources to mitigate the multiple risks arising from data protection non-compliance: a challenge presented by the work-time paradox.

High level recommendations

The participants in the workshops discussed that a risk-based prioritisation of GDPR activity will be necessary. If this is to form the basis of LSBU’s GDPR Vision, naturally it would be wise for LSBU to define what ‘risk’ actually means and then find where its substantial risks lie, so they can be meaningfully addressed and triaged in the coming months.

The idea of risk encompasses many different things. In the context of a GDPR programme, this includes (but is not limited to) **‘legislative compliance risk’**, which means the risk of not satisfactorily completing the compliance activities set out in the legislative text; **‘operational risk’**, which means the risk of business operations not being conducted in a way that delivers on the rights, principles and architectural requirements of a good approach to data protection; **‘regulator risk’**, which means the risk of coming into conflict with the regulatory system, including the risk of regulatory investigations, enforcement proceedings, penalties and sanctions; **‘delivery risk’**, which means the risk of not being able to find adequate internal and external support to deliver on the requirements of the GDPR; **‘data subject risk’**, which means the risk of not being able to satisfy a request, requirement or complaint of an individual; and **‘reputation risk’**, which means the risk of damage to the organisation’s brand and reputation. Plainly, these risk areas are, or can be, interwoven and interconnected, but not necessarily so. For example, it would be possible to fall foul of the regulator without suffering major brand damage. It is equally possible to be technically non-compliant with the legislation without coming to regulatory attention, or to be fully compliant with the legislation, while still having weak operations that may not stand up to the scrutiny of a determined individual. Another way of looking at it, would be to say that a ‘box ticking’ approach to the legislative requirements may not result in the termination, treatment or transfer of risk. Worse still, it is possible that a box ticking approach leaves other risks unknowingly tolerated.

We understand that these are complex ideas and so we are constrained to say that our recommendations cannot address all risk areas, hence why we have concluded that LSBU will be operating unlawfully to a degree in May 2018. Instead, we have tried to identify a balanced portfolio of activities that will work across many risk domains. However, there is a natural bias towards legislative risk, because, after all, the GDPR provides the first yardstick against which organisations will be judged, as well as the foundation stone upon which the wider set of risks can be managed.



Formulate LSBU's GDPR Vision and Strategy

It is recommended that LSBU agree a Vision for the GDPR programme. The vision should identify LSBU's objectives, approach and timelines. Agreeing a vision and strategy will ensure the appropriate direction of the GDPR programme and will support the implementation of a prioritised series of activities (based on risk) designed to effect meaningful and measurable change across LSBU.

Once the vision is agreed, we recommend that LSBU formulate a detailed GDPR "Strategy" as a matter of priority. In the run up to May 2018, it is likely that LSBU's partners and perhaps users will start asking challenging questions related to LSBU's GDPR readiness.

Without wishing to pre-empt the outcome of these exercises, it might be appropriate for LSBU's GDPR vision and strategy, which should be published online as part of their data protection policy, to cover LSBU's commitment to the GDPR, stating that LSBU has an implementation programme underway, explaining that LSBU will focus on the biggest risk areas for personal data in the first instance, which are where there are the greatest risks of harm (pecuniary damage and significant distress) to individual and to the University's brand and reputation. The GDPR strategy should contain sufficient detail to satisfy LSBU's partners/students, but not be so prescriptive as to bind LSBU to impossible outcomes. Ideally, we would expect the content of any external facing statement to align with the content of the GDPR strategy.



Governance and Resources

GDPR programmes typically require proper governance and ownership. LSBU have hired external support to ensure there is ownership for the programme and has the most senior leadership in the University as sponsorship. To ensure that the programme is successful in the long run LSBU will have to appoint a lead for Data Protection, the previous DPO had left the University between the Readiness Assessment and Special Characteristics workshop, this role should be filled to ensure once May 2018 comes around BAU activities can be picked up by the lead or data protection.



Requirements list

A helpful exercise would be to map the GDPR requirement to each area of the business where the requirement will be managed, so that LSBU understand which principles, rights and 'build requirements' (e.g. DPIAs, DPOs, DPbD) apply. It is important to establish the situations where compulsory legal requirements exist. For example, the data portability right applies only to consent and contract based processing. Completing the GDPR mapping exercise will ensure LSBU do not waste time building solutions that are not strictly necessary. This mapping activity will form part of the programme scope requirements document which is completed at the start of the programme. It is recommended that each article of the GDPR be documented in a matrix indicating what area of the business the article affects and the obligation of that business area to demonstrate compliance.



Records of Processing

Article 30 supports the idea of 'data mapping' and it is highly predictable that data maps will be sought during regulatory investigations and inquiries.

LSBU should perform a data mapping exercise in order to understand and assess its existing personal data landscape. This activity will support in understanding the various flows of personal data within LSBU as well as what personal data is shared with third parties and partners. By assessing what types of personal data is collected and the purposes for this collection, LSBU will be able to ensure that the correct lawful basis is being adhered to and that any future changes to systems or processes occur with the understanding of upstream and downstream effects.

At the same time, it is important to take a balanced and proportionate approach, bearing in mind that there are not yet any binding authorities that help us to understand the nature of the burden. However, we are convinced that some organisations have taken an unnecessarily 'hard' approach to this task. In the circumstances currently facing LSBU (time and resource constraints in particular), we recommend a light approach. Moreover, the mapping exercise should support the creation of the risk registers, so the data has to be intelligible and usable.



Identify which risks matter the most

Given that LSBU has expressed a desire to take a risk-based approach to the GDPR, it is critical that it forms a coherent view on which risks matter to LSBU the most and therefore which risks to address first. Such as Student Records, Global partnerships and Information Security. As already suggested above, LSBU could decide to first tackle those risks which may cause pecuniary loss or damage to data or a risk of significant anxiety. Any prioritisation of loss or damage-based risks should take place together with consideration of the 'hot topics' that are of interest to LSBU.

Plainly, this requires LSBU to build a risk register (which is an implied requirement of Article 24 and Article 35), against which risks are rated by reference to likelihood or occurrence and impact, with decisions about termination, treatment, transference or tolerance.



Conduct a gap analysis of your data protection paperwork

LSBU has a number of informal processes in place for data protection. However adequate documentation that can be produced on request is one of the key elements to complying with the accountability principle (Articles 5 and 24), this requires that organisations not only comply with the GDPR, but are also able to demonstrate compliance. Regulators aside, LSBU's global education partners may also want to have sight of its documented policies, procedures, notices and contracts as part of their due diligence procedures. Moreover, in a 'quality assurance' sense, the beginning of the journey to QA is the creation of a written system of rules for the performance of business operations.

We recommend that LSBU reviews its whole suite of data protection and privacy documents to identify which parts of its paperwork require improvement. A good quality data protection system contained in paperwork can act as a shield against many forms of adverse scrutiny, including many forms of regulatory investigation. It is our assessment, based on our tracking of the regulatory cases, that most instances of regulatory investigations and inquiries are resolved by reference to the quality of the paperwork that the organisation can produce. In other words, in a regulatory sense the paperwork provides the first line of defence.



Conduct a technology functionality gap analysis

Creating a requirements list will help LSBU to understand which obligations should be integrated into the technology stack. Obviously, security measures need to be integrated, but a secure technology stack in isolation will not meet all of the requirements of the GDPR.

Armed with a full list of requirements, we recommend that LSBU should conduct a technology functionality gap analysis, to understand the extent to which the principles and rights requirements of the GDPR can be delivered by the incumbent technology stack itself: we predict a much more heightened focus on the operational adequacy of the technology stack under the GDPR than compared with the current and previous data protection regimes.



Methodise the new privacy 'big pillars'

Perhaps the most important innovation of the GDPR is that it has an inbuilt 'how to guide' for delivering operationally good outcomes for data protection, which we sometimes call the 'Build' requirements. This consists of the accountability requirement (Article 5), the policy requirement (Article 24), 'privacy by design' (Article 25), data processing records (Article 30), breach notification (Article 33 & 34), DPIAs (Article 35) and Data Protection Officers (Article 37). It is a racing certainty that organisations' responses to these requirements will be tested once the GDPR is in force. Naturally, LSBU will need robust responses to any questions asked in regards these requirements.

Generating these robust responses means moving the legislative requirements into workable methodologies, which of course means that there will need to be piloting activities. If done properly, piloting will enable LSBU to deliver credible answers to these legislative compliance obligation as well as aiding the freezing of the risk.



Start to stress test your data protection framework

To date, LSBU has not fully examined the operational effectiveness of its data protection framework. Therefore, LSBU does not know how the resources it has in place would handle the additional strain placed on it due to a data breach, or, indeed, any other challenge relating to data protection principles and rights (such as subject access request challenge). PwC considers that the data protection rights of data subjects will be significantly better known by the time the GDPR applies in May 2018. In our view, this will place greater demands on organisations as the GDPR rights come to be exercised. As well as highlighting areas for improvement, formal exercises will also provide LSBU's employees with training around how to respond to events and ultimately provide them with a 'safe' environment in which to test their reactions and solutions.

Therefore, we recommend that the operational elements of LSBU's data processing activities will need to be stress tested to see how they would withstand adverse scrutiny. The adverse scrutiny test will identify potential future stress areas, but obvious ones include:

- Handling Personal Data Breaches and breach notifications.
- Handling complaints coming in about marketing activities.
- Handling regulatory investigations, where the regulators use their investigatory powers.
- Handling new Data Subject Rights requests.
- Handling politically motivated challenges, where data protection is weaponised.
- Handling employee challenges, where data protection is weaponised.



'Freeze' your risk and identify a suitable pilot

The GDPR requires entities to address legacy and future risks. Ideally, LSBU will avoid the structures of new data processing activities becoming part of its legacy risk environment. To get to that point, LSBU should first identify new or future data protection activities that involve personal data processing and privacy risks (e.g. Student Records System); LSBU should then apply a 'temporary' or holding compliance programme to those activities which covers the key Principles, Rights and Build requirements in the GDPR, or in some instances acknowledge that if the programme does not address data protection that this will result in compliance failures at deployment.

The implication, of course, is that delivering compliance in a new area will act as a pilot scheme for the wider change programme, helping LSBU to understand the feasibility of the temporary structure being rolled out more generally, including to legacy risk areas. Pilots should certainly cover the new privacy 'big pillars'.



Leverage success and learn the lessons of failure

Programme success will depend, in part, on gaining efficiencies. LSBU should consider prior situations of business transformation, to understand what has worked and what has failed. Successful programme approaches should be repeated, where possible, and the failures avoided. This is definitely worth the investment of time to think through.

Understanding the cause of problems during business transformations or in business processes may be insightful. Questions to ask would include why the process was not working properly or why wider business engagement is not achieved?



Quick win and no regret activities

When the effort of changing a written policy framework is compared with the effort of changing a technology stack, it will be obvious that the former is quicker in a relative sense than the latter: a single person could write a new data protection policy over a weekend, but technology transformation needs a team of internal and external experts and a longer runway. Therefore, policy refresh might be considered to be a quick win and no regret activity. Likewise, the creation of data maps and methodologies for risk assessments etc.

LSBU should think laterally about what else can be done along these lines. For example, if the Article 28 requirements are considered, it will be clear that technical compliance may be hard, because the procurement and contractual frameworks at both sides of the contract may not yet be conducive to delivering quickly on the GDPR requirements. However, if legislative compliance is hard, risk mitigation might be easy. So, LSBU could send notices to all of its third parties and partners to remind them of their duties to act responsibly. This would be a quick win, no regret activity that has a meaningful effect on risk reduction in the wider sense. The creation of notices and information boards (e.g. intranets) and simple awareness raising programmes will have a meaningful effect on LSBU's risk profile, so will putting GDPR training into new employee inductions, as will the appointment of 'GDPR Champions'.

DRAFT

LSBU's Special Characteristics

Special Characteristics Workshop

The Special Characteristics Workshop focused on the following three areas:

- What does 'data privacy' mean to LSBU?
- What does 'risk' mean to LSBU?
- What does 'good' look like to LSBU?

In addition to the sessions noted above, one of the key purposes of the Special Characteristics Workshop was to contextualise the gaps identified by the R.A.T, to help identify which areas ought to be tackled first this was achieved by presenting a sample GDPR road map whereby LSBU discussed and debated the existence of activities and workstreams, including expectations for when these will be delivered.

The following business units and functions were represented at the Workshop:

- *Human Resources*
- *Health and Safety*
- *Corporate Affairs*
- *Executive Office*
- *Finance*
- *Marketing, Admissions and Communications*
- *ICT*
- *Procurement*
- *Student Support and Employment*
- *International*

Themes

We identified a number of themes from the Special Characteristics Workshop:



What does 'data privacy' mean to LSBU?

The first discussion during the Special Characteristics Workshop concerned the participants' understanding and opinions on the meaning of data protection and privacy to LSBU. We have summarised the key talking points below:

Trust and Reputation

Student Trust Participants highlighted that student trust in LSBU is one of their highest priorities. Student data is the largest data set held and managed by LSBU, due to other legislative requirements LSBU does not delete this personal data. In addition to all the personal data stored on LSBU systems there are many touch points during the student journey, in some cases personal data is collected on behalf of LSBU by other education bodies and third parties, but throughout the student lifecycle many various departments interact with student data, such as admissions and enrolment, housing, lecturers and other students where they are employed by LSBU, all the way to Alumni services. This increased landscape where student data resides can result in student data being susceptible to theft and authorised access and disclosure.

Employees and students are required to sign up to LSBU's data protection policy to confirm that they will protect personal data. LSBU had indicated that students and employees are 'hypothetically' well informed of how to protect personal data. There is an expectation from both staff and students that there is a duty of care towards student data.

Integrity and Confidentiality

Protecting personal data Participants mentioned that due to technology restrictions not all employees of LSBU receive LSBU equipment such as laptops and tablets. There are cases in the University where employees will purchase their own IT equipment or bring in their own devices and then connect to LSBU corporate networks to access systems holding personal data.

There was a strong requirement for standardised process in both requesting a laptop and securing personal devices that are used for work relating to the University. The participants are working towards compliance but want stronger enforcement across the University where employees and students use their own devices to access personal data, this also includes where students are provided a LSBU email address which is part of the corporate network, there is very little to no policy or training provided to students, therefore if a malware attack was targeted at students this could infect the wider LSBU network.

Improving relationships and embedding data protection as a value add

Employer Relationships The participants were keen to have a unified approach towards data protection and how it is executed across the University. There was a belief that policies already implemented need to be reviewed as some issues have not been addressed, this includes strengthening policies and procedures to ensure that these cover the necessary GDPR provisions.

In particular, most participants were unaware of the appropriate grade in which staff were able to work from home in accordance with the policy. It was also communicated that the Executive would prefer an ethical approach to the GDPR as opposed to a rules based approach to data protection.

LSBU's core business is personal data

Protecting Crown Jewels It was agreed by participants that due to their status in the Higher Education industry, LSBU has a heavy focus on data. By collecting and sharing data, LSBU are able to more accurately market to their consumer base and continue to grow their business. Participants remarked that although LSBU's students had high expectations of LSBU, they are unlikely to be aware of how much and for how long their data is retained. However, LSBU do not receive many data subject access request and the number of complaints pertaining to data

breaches is low, this equates to a low protection education across the employee and student base which will change after May 2018.

Due to LSBU being in the Higher Education sector, it would be very easy for there to be a spike in DSAR's and complaints if students feel that their data is being mistreated. This is a particular risk under the GDPR as it will be easier for class actions lawsuits to be carried out. However, as LSBU's competitors undertake a number of profiling and marketing activities to engage more students and partnerships, LSBU would need to ensure that their data protection practices and compliance activities would not leave them at a disadvantage in the market. LSBU will need to ensure that prospective students would have faith in joining LSBU that LSBU would protect personal data.

Data Protection as a route for reform and as a differentiator

Compliance versus Benefit Participants acknowledged that the GDPR was a further regulatory and compliance obligation on LSBU that would require them to reconsider the vast majority of their operations and relationships. However, participants voiced that although their privacy practices are not the best in their industry, the GDPR provides an "opportunity to mature" their standards and consider privacy at the forefront of their processing activities. LSBU understood that by having a clear understanding of what data they hold and where it is held, they can streamline procedures and in some cases their working day. By understanding this, when LSBU encounter audits or even in some instances subject access requests, they can provide an example of data mapping to pinpoint what information is held where and effectively extract the data for the subject request.

LSBU need to have at least a degree of transparency when it comes to student's data. It was discussed during the workshop that if students felt like they were being lied to or misled then this could increase the number of complaints or in severe cases, the University being reported to the educational board. It was reiterated throughout that student's trust was paramount and any misunderstanding could be negative for the LSBU brand.

Participants wanted to emphasise that data protection had its advantages, like providing comfort to students when they join the University, especially if they enter an international transfer.

What does 'risk' mean to LSBU?

The next topic for discussion was the participants' views on the meaning of risk. The following principle themes arose during this discussion:

Risk due to GDPR non-compliance

Getting the basics right

The primary risk discussed by the participants was that of non-compliance. If this risk could not be addressed and remediated then there would be little hope in addressing any other risks which might flow from it. There was discussion that LSBU could fail on data protection just by simple errors such as the example provided where a student personal data could be shared erroneously by placing student data into internal mail and not using alternative secure processes provided by the University. It is believed that the current data protection training needs to be updated to include more references to GDPR and data protection, and include scenarios to help employees associate data protection risks to their own environment.

Risk of brand damage

International repercussions

The primary risk discussed by the participants was the risk of reputational damage to LSBU's brand, especially given its student population.

For LSBU, participants agreed the business' dealt with high quantities of data but the University did not always have to gain consent to use the data as it falls under public interest as personal data is collected as part of a public requirement. However, it was accepted by participants that a data breach would have an impact on LSBU's and its partners' reputations. Difficulties in recruiting employees, creating new relationships abroad and the status in the education sector were all perceived as likely consequences of a personal data breach.

Participants appreciated that LSBU needs to conduct data analytics in order to develop as a business and institution but would have to be transparent as in doing so it runs the risk of upset.

Another key concern for LSBU participants around risk of brand and reputational damage was not only in the eyes of future students and Alumni but with their international relations partners who provide funding, research grants and actively recruit students for LSBU. The LSBU international office works alongside various organisations in a wide range of countries, and if the LSBU brand was damaged then international organisations may not enter into or continue with future partnership. This risk would also come with financial implications as international student fees play a large part in the funding and support of the University.

Structure of the programme

Failing timelines

Participants believed that the lack of timescales, milestones and ownership of workstreams could pose a risk to LSBU as the implementation needed for each stage of compliance lacks structure. It was also recognised that there was a delay in receiving the appropriate sign off for major projects, impacting the roll out and the validity of the programme.

Related to this issue is the risk of how to keep staff members engaged and up to date with the implementations happening throughout the University as many employees feel that information does not filter down in a timely manner. The question was also raised about building these new compliance checks in to training for new staff currently being employed as well in the future.

A significant point highlighted by the participants related to the cost implications of implementing the GDPR. Whilst it was raised during the workshop it was not formally discussed. Under programme governance, the participants linked cost to the scope of

the project and the responsibility of the individual business units to determine how LSBU will fund this project. The issue of finance is key to the deliverance of the project as it includes how project milestones, deliverable dates and resources are implemented. It is advised that LSBU reviews each business unit to determine the scope and cost of implementing their GDPR programme across the University

Risk of losing students to competitors

Market differentiator

For LSBU, a significant concern amongst the participants was the risk of business loss caused by inadequate data protection implementation. Under the GDPR, it will be easier for students to take action against the University. There is an awareness that Universities rankings are published and made widely available, so a public personal data breach would be a concern for perspective students and could impact LSBU position in published University rankings or published in news articles linked to the University. LSBU may therefore loose students to their competitors as they are seen to have a lack of concern of their student's personal data.

Participants articulated that data protection considerations needed to be balanced against student trust and the realisation of what could be achieved in 7 months.

Due to their status as a University, LSBU have various contacts and partnerships overseas to be able to provide international transfers for both foreign and UK based students. There is acknowledgment, to a degree, the risk of having international relationships can cause. Questions were raised in regards to who controlled the data as information is collected by both LSBU and the partnered companies and suppliers, for example the British University of Egypt. There was uncertainty surrounding the agreements with suppliers that are currently in place as it was unclear what rights third parties have over LSBU student's data, the timeframes in which to notification should occur and who should fulfil a subject access request.

There was an indication that there is a lack of knowledge regarding the data held about international students and the life cycle of that data. This was especially highlighted as there was no clear understanding of data being transferred to LSBU from the EU, where it is stored, how it is handled and how it is processed. The international office were aware that they would have to review and update their current contract with suppliers to become complaint under the GDPR.

What does “good” look like to LSBU?

The characteristics of a “good” privacy programme can mean different things to different organisations. We have included some examples of these below.



From this session, PwC observed the following themes from participants with regards to what they felt “good” would look like to LSBU:

Good is “approaching the GDPR in a smart way”

Participants articulated that it was important that LSBU understood what it means to be compliant in the areas that matter most to students, employees, regulators and third parties. Participants articulated that it may not be possible for LSBU to be fully compliant across all of the GDPR obligations, nor within the May 2018 deadline but understood what their biggest risk areas were. The participants recognise what ‘good’ looks like but due to a lack of defined procedures, policies and technologies it is hard to implement across LSBU. There was an understanding that there needs to be a methodological approach from top down for good practices to transpire.

Good is “knowing where the data comes in to the business and understand where it is going”

Participants felt that “good” would include having clarity over what data was being held in different systems by LSBU, who had access to it, how long it would be retained for and who they were sharing it with and why.

Good is “embedding data protection awareness into what we do”

A significant theme discussed was raising awareness and educating LSBU employees on GDPR and data protection good practice in order for it to be embedded across the organisation. This would range from employees having received data protection training, understanding who the data stewards are and knowing where to send complaints or DSAR’s to. At present, employees have varying knowledge of data protection but LSBU have already begun to implement training via their learning and development team to bring all the University populations to the same level.

Good is “*having leadership for Data Protection*”

From a data protection perspective, LSBU believes that there needs to be ownership of the data that LSBU holds and processes. Whilst there is recognition that there is no central team who “owns” the data protection process, there is a perception that there will be a team to oversee it. There was concern that data protection would be approached as an add-on to employees day jobs and that there would be no consistency in LSBU’s approach to compliance. The risk of the lack of consistency and harmony across the University could possibly lead to breaches and derailment of the overall programme.

Although LSBU are in the process of recruiting for a Data Protection Officer, the participants wanted to reinforce that whilst the DPO will establish the framework each individual function will need to take ownership of future policies and procedures and ensure they are implemented.

DRAFT

Appendix 1: LSBU Roadmap

Appendix 1: LSBU's Recommended Roadmap

The approach for the GDPR Road Map is to enable LSBU to make a start on areas of priority, as well as identifying what would put LSBU ahead of the curve and limit the amount of regulatory scrutiny. LSBU would need to be seen to at least have a programme for achieving GDPR compliance by May 2018 based on their greatest risk, this is represented by the various work streams highlighted in the Road Map below. The road map was developed with LSBU during the special characteristics workshop.

In order to drive forward the GDPR compliance programme, LSBU will first need to ensure it assigns the appropriate resource and budget to meet the demands of the new regulatory regime. The amount of work required towards compliance in the limited time available makes this a key area for consideration. Depending on the approach that LSBU takes to the implementation of its GDPR programme, budget may be required for new internal hires and external support, to deliver review-based activities (data mapping, training and awareness programmes, gap analysis etc.) and new data protection systems (policies, procedures, processes etc.).

		2017		2018			
Workstreams	Business Function	October - December		January - March		April - June	July – September
GDPR Programme Governance	Data Protection			Agree and Define			
Governance, Roles and Responsibilities	Data Protection			Agree and Maintain			
Gap Analysis	Corporate Governance / Legal			Document and Approve		Update and Communicate	
Third Party Management	Information Security			Assess Gap and Implement		Implementation and Monitoring	
Breach Response	Procurement / Legal			Assess Gap and Update		Implementation and Monitoring	
DPIA and DPbD	Legal / Projects			Assess Gap and Update		Implementation and Monitoring	
Data Mapping and Usage Requirements	Data Protection / IT			Scope, Test and Document			Ongoing monitoring and Updating

1. Create a GDPR Programme Management Office

In order for LSBU to embark on a full GDPR compliance programme, effective project and programme management is required to ensure that the right resources are allocated with the necessary budget. Once established, the programme management office should create a list of GDPR requirements, leverage successful business change processes from elsewhere in the business, take steps to freeze LSBU's risk and consider quick wins and no regret activities, as well as wider GDPR activities. In addition, the programme management office would include setting milestones, key deliverable dates and tracking project spend and resource availability.

The purpose of a creating a GDPR requirements list is to ensure that LSBU carries no ambiguity about its legislative obligations within the GDPR and to minimise the risk of transformation effort being expended on unnecessary activities. Utilising previous business change success stories can increase efficiency and the prospects of success for the GDPR programme. Classic theories of Quality Assurance require organisations to learn the lessons of failure. Note, also the scheme for the imposition of administrative fines in Article 83.

Freezing risk can assist in identifying any forthcoming initiatives that can be put on to a new data protection platform in order to crystallise LSBU's risk and restrict the development of risks in new data processing activities. For example, major innovations or projects (such as the Student Records System) could be used to pilot a 'temporary' or holding compliance programme (e.g. incorporating DPIA, or Privacy by Design). Provided the programme is working to LSBU's satisfaction, LSBU may then want to consider if it is feasible to deploy the programme to address legacy risks.

Finally, highlighting quick wins and no regret activities will allow low effort work to begin almost instantly, regardless of the risk positions. For example, Article 28 will likely require that LSBU puts in place new contracts with data processors. Pending the resolution of that problem, LSBU might simply send notices to partners about what is expected of them. Although this approach might not deliver strict legal compliance with Article 32, it delivers risk mitigation.

These activities are not linked directly to RAT domains, but are included to ensure that good programme governance is established to ensure success.

GDPR Programme Management Office:			
#	Activity	Tasks / Description	End State
1.1	Document GDPR governance programme function so that necessary operational change is delivered	<ul style="list-style-type: none"> Define and appoint dedicated project team to manage the GDPR transformation programme. Identify cross business function support (i.e. Information Security, IT) to act as contributors and owners of activities. Publish a stakeholder list of points of contact in LSBU who would be responsible for effecting change and be a point of call for the programme. 	<ul style="list-style-type: none"> Allocated GDPR compliance programme resources
1.2	Determine quick wins	<ul style="list-style-type: none"> Identify quick wins (these can include, drafting policies and procedures, formalising vision and establishing BAU governance) 	<ul style="list-style-type: none"> Documented quick wins

GDPR Programme Management Office:			
1.3	Define key metrics and milestones	<ul style="list-style-type: none"> • Allocate programme resources to various work streams and activities. • Define and determine key milestones for tracking programme status and workstream completion, these should include setting dates for drafting, approval and implementation of documentation, and implementation of activities. • Define and agree on key performance metrics for programme leads and workstream leads to be measured against. • Implement regular reporting and status planning sessions to ensure programme timelines are being adhered to and budget is being measured. 	<ul style="list-style-type: none"> • GDPR project plan (including milestones, delivery start and end dates)
1.4	Assess impact on GDPR compliance programme from other internal factors	<ul style="list-style-type: none"> • Assess all ongoing or upcoming projects or programmes that would affect EU personal data or GDPR compliance such as upcoming technology or processes upgrades, new research or collection of additional special categories of personal data. • “Freeze Risk” (such as not proceeding on contracts or programmes which are higher risk) by either re-defining projects and programmes or supplier contracts, ensuring that no further risk to GDPR compliance is initiated. 	<ul style="list-style-type: none"> • Risk prioritisation of upcoming or future programmes, projects or outsourcing arrangements

2. Define Governance structure (including roles and responsibilities)

LSBU had indicated that it has low (but developing) maturity regarding privacy and GDPR governance. This workstream, and its associated activities, will develop who within the LSBU organisation is accountable for GDPR and data protection related issues and will ensure that employees within LSBU have designated roles and responsibilities to support the compliance programme. To ensure ongoing compliance to the GDPR, data protection roles should ideally be formally defined within existing roles and should be measured to ensure LSBU is achieving its desired vision.

A key priority for LSBU should be to designate appropriate ownership of the GDPR programme. Remedying this will be critical for:

1. Successful business transformation.
2. Helping LSBU to withstand serious cases of adverse scrutiny which will closely examine its governance structures, roles and responsibilities.
3. Ensuring LSBU’s legal compliance obligations are met (for example the requirement to appoint a Data Protection Officer where certain triggers are met (see Article 37)).

RAT results:

RAT domain	RAT question	Maturity
Governance	Is your data protection programme sponsored by executive or board level management?	2

RAT domain	RAT question	Maturity
	Is a steering committee in place to provide strategy and direction to your data protection programme?	1
	Does your data protection programme have leadership support within the business?	2
	Have you assessed the GDPR requirement to appoint a DPO?	2
Roles and Responsibilities	Have data protection roles been deployed within the business?	2
	Have information security roles and responsibilities been reviewed against the GDPR personal data security requirements?	2
	Have information governance roles and responsibilities been reviewed against the GDPR personal data management requirements?	1
	Is there alignment between the various functions responsible for elements of data protection compliance (data protection, information security, information governance)?	2

Recommended work streams:

Governance, Roles and Responsibilities			
#	Activity	Tasks / Description	End State
2.1	Determine the organisational structure and reporting lines for Data Protection.	<ul style="list-style-type: none"> Document the current organisational structure and reporting lines for data protection and decide on the most appropriate model (centralised / Hybrid / decentralised model). Define the structure of the GDPR function who would be responsible for business as usual activities, including how this interfaces with the business. Update and obtain sign off on defined structure from required committee(s). Document / update terms of reference for Steering Committee including the GDPR committee. 	<ul style="list-style-type: none"> GDPR governance structure and reporting lines defined.
2.2	Identify and appoint data protection champions in the business.	<ul style="list-style-type: none"> Define the roles and responsibilities for Data Protection champions in the business. This responsibilities should include (1) ensuring that employees in their immediate scope understand the need for good data protection practices and are adhering to policy. (2) Passing on good practice both up and down the chain of command. (3) 	<ul style="list-style-type: none"> Data Protection champions appointed and briefed. Ongoing Data Protection forums.

Governance, Roles and Responsibilities

- | | | |
|--|--|--|
| | <p>Reporting potential data protection / security incidents and bad practice so that it can be addressed.</p> <ul style="list-style-type: none">• Formally identify appropriate individuals to represent all business units / functional areas (i.e. Information Security, IT, Finance, HR, Operations)• Update employee contracts and role descriptions to include data protection responsibilities.• Define KPI's and metrics for performance for data protection champions (i.e. Compliance Management, Data Quality etc.)• Define and document RACI for all Data Protection responsibilities and who would be “responsible, accountable, consulted and informed”. Ensure all named employees are aware of the requirements.• Formalise the ongoing Data Protection forum for data protection champions to brief them on roles and responsibilities and key data protection messages (can be included into wider data centric conversations to ensure that these roles are not compliance driven but operational) | |
|--|--|--|

3. Prepare “paper shield” (data protection policies and procedures)

This workstream will ensure that system deficiencies are identified in order to produce the necessary paper shield. In some cases this will involve creating or updating existing documentation, or leveraging existing policies, operating standards and procedures to form part of the paper shield. Participants at the Special Characteristics Workshop highlighted the importance of getting data protection policies and procedures in order and updated for the GDPR to ensure that LSBU can provide adequate documentation on request from regulators (i.e. in compliance with the “accountability principle” of the GDPR).

This activity involves a review of LSBU’s paper-based policies, procedures, notices, contracts, and so on, that it has in place to give effect to the GDPR’s requirements.

The purpose behind this activity is:

1. To facilitate business transformation – written rules are embedded into operations for quality assurance purposes.
2. To help LSBU meet the demands of regulators and other scrutineers – The theory of systems based regulation tells us that players look at the paper system first.
3. For legal compliance (in particular Articles 5, 24, 30, 32 and 26)

RAT results:

RAT domain	RAT question	Maturity
Policies	Do you have a data protection policy?	2
	Do you have an information security policy?	2
	Do you have an information governance or management policy?	1
	Do you have an information classification and handling policy?	1
	Are procedures in place to ensure policy provisions are incorporated into business processes?	2
Rights	Do you have policies and procedures for subject access requests?	2
	Do you have policies and procedures for individuals to raise issues or complaints about how their personal data is processed?	1
	Do you have policies and procedures for individuals to raise issues and complaints about direct marketing or profiling activity?	1
	Do you have policies and procedures for assessing and complying with requests for erasure of individuals' personal data?	1
	Do you have policies and procedures for data portability?	1

Recommended work streams:

Prepare “paper shield” (data protection policies and procedures)			
#	Activity	Tasks / Description	End state
3.1	Develop a GDPR “paper shield” framework (all documentation necessary to satisfy paper shield)	<ul style="list-style-type: none"> Assess what documents will need to be included as part of the paper shield. Create a comprehensive list of all documentation necessary to satisfy paper shield. Assess existing standard operating policies and procedures and identify existing contracts and transfer agreements. 	<ul style="list-style-type: none"> Documented GDPR policy framework and contract list
3.2	Assess gaps between required documentation and existing documentation and document	<ul style="list-style-type: none"> Perform gap analysis of paper shield and existing LSBU policies, procedures and standards. Identify what documentation should be created which does not currently exist. Identify what existing documentation can be leveraged. Identify what existing documentation requires amendments to satisfy new requirements. Design a template and format or use existing templates for GDPR policies, procedures, standards and contracts. Document or update all required GDPR policies, procedures, standards and contracts. 	<ul style="list-style-type: none"> Documented paper shield gap analysis
3.3	Perform ongoing review and update of policies and procedures	<ul style="list-style-type: none"> Review policies, procedures, standards and contracts (in line with defined review cycle) on an ongoing basis to ensure applicability against current risk profile, compliance and threat landscape. Update policies, procedures, standards and contracts as required. Tools and technologies could be used to track the status of documents and remind owners when updates are due. Communicate and educate staff on new documentation. 	<ul style="list-style-type: none"> Documented new and updated GDPR policies, standards, procedures and contracts
3.4	Perform adverse scrutiny testing on areas of greatest risk	<ul style="list-style-type: none"> Determine LSBU’s adverse scrutineers (set of actors who can raise regulatory concern over data processing operations i.e. ICO or data subjects). Determine areas of the business and scenarios where there is increased concern from these ‘adverse scrutineers’ (e.g. data subject rights, complaints management, and personal data breach). Perform scenario based testing in these areas of concern to ensure that in the event of a situation arising that LSBU would be best placed to respond and remediate known issues. 	<ul style="list-style-type: none"> Documented Adverse Scrutiny scenarios and gap analysis

The associated technologies which will support data subject rights from policies and procedures have not been included into the activities, these must not be overlooked and should be implemented once the necessary documentation and processes have been defined.

4. Records of Processing

Data mapping needs to be completed across LSBU to assess and understand not only how data interacts with systems but specifically the flows of European personal data and the processing operations. This is to provide a full view of the personal data processed to ensure that all data protection risks are identified globally and there is clarity on how personal data is processed. Once a full view of the various systems is understood, additional controls can be implemented to ensure that data in non-applicable systems is removed or stored in LSBU's sanctioned systems.

The purpose here is to ensure that LSBU understands core information about its processing activities, which together with the Requirements List will enable LSBU to make informed decisions about the nature of its risks and the necessary treatments. Data Maps are required by Article 30, in most cases.

RAT results:

RAT domain	RAT question	Maturity
Registers	Do you maintain a register of your personal data processing operations?	1
	Do you have an information asset register and retention schedule?	2
	Have you documented flows of personal data (including capture, access points, transfers and disposal)?	1
	Do you maintain a register of recipients of data such as data processors, other controllers including public authorities and other third parties?	1

Recommended work streams:

Data Mapping			
#	Activity	Tasks / Description	End state
4.1	Perform a Data Discovery Exercise and Data Mapping	<ul style="list-style-type: none"> Run workshops with necessary stakeholders to identify the types of relevant personal data processed. Perform interviews with employees to understand processing and the quantity of this data. Determine existing IT infrastructure requirements and the capability to support and perform data discovery. 	<ul style="list-style-type: none"> Documented IT systems mapping and data maps

Data Mapping			
		<ul style="list-style-type: none"> • Support and clarify manual identification with tools to discover further personal data and special categories of personal data. • Analyse the scan results (if tools are used) and document action plans with internal stakeholders. • Run workshops and interviews with relevant stakeholders and develop/update IT Systems data maps to understand where personal data is processed and stored. • Develop EU personal data flow maps. • Analyse the results and document action plans with internal stakeholders. 	
4.2	Identify data transfers	<ul style="list-style-type: none"> • Assess whether EU personal data is being processed outside of the EU. • Ensure the appropriate transfer mechanisms are in place for transfers of EU personal data. • Document the transfer mechanism relied upon to legitimise the transfer of EU personal data (i.e. Contracts, Data Transfer Agreement, Privacy Shield). • Update data maps to reflect transfers and their mechanisms. 	<ul style="list-style-type: none"> • Documented personal data discovery included on data maps
4.3	Build Article 30 Record of Processing Activities	<ul style="list-style-type: none"> • Build a register to meet the requirements of Article 30, namely one which sets out: • Name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; where possible, the envisaged time limits for erasure of the different categories of data; where possible, a general description of the technical and organisational security measures referred to in Article 32(1). 	<ul style="list-style-type: none"> • Documented Article 30 records of Processing register

5. Data Usage and Handling Requirements

This relates firstly to LSBU's ability to assess and demonstrate that each instance where it processes personal data is grounded on one of the specified lawful bases for processing personal data, for example, consent, and performance of contract or compliance with a legal obligation. The results of LSBU's assessment of the lawful bases and the means under which the processing will be deemed lawful (e.g. through consent) should be documented to meet

LSBU's accountability obligations to the GDPR. In addition other GDPR principles should be defined, such as purpose limitation, data minimisation and data accuracy. It was noted by LSBU that informal processes exist around data minimisation and accuracy, which have developed due to customer interactions.

In addition to assessing and defining the necessary lawful basis for processing personal data, is essential to review the existence of permissions received in relation to direct marketing and whether these permissions are lawful and can be relied on as it relates to the requirements of the GDPR and e-privacy requirements.

RAT results:

RAT domain	RAT question	Maturity
Lawfulness, fairness and transparency	Do you have processes for assessing the lawful bases of new personal data processing activities?	2
	Do you have processes for assessing the lawful bases of new processing activities involving sensitive personal data?	2
	Are you planning to review the lawful bases for processing employee data?	2
	Where consent is relied on, are those consents documented?	2
Data Minimisation	Do you have procedures for assessing the extent to which personal data is required to achieve the processing purpose(s)?	1
Accuracy	Do you have procedures for ensuring personal data are accurate and where necessary kept up to date?	1

Recommended work streams:

Data Usage and Handling			
#	Activity	Tasks / Description	End state

Data Usage and Handling			
5.1	Implement / Update Data Lifecycle minimum requirements	<ul style="list-style-type: none"> Assess data lifecycle and data journey and identify all touch points where data protection risks exist as a result of the data discovery mapping. Assess all personal data processed as part of data discovery and mapping and assess the lawful basis for processing (make a determination whether the existing lawful basis is correct option). Where necessary implement safeguards to ensure that least amount of personal data is processed / collected in order to satisfy and demonstrate the 'minimisation principle'. Assess data in existing systems and technology and cleanse data and remove duplication to ensure only all necessary data is retained in the LSBU environment. Where necessary, implement technical safeguards to reduce collection of special categories of personal data and children's personal data. 	<ul style="list-style-type: none"> Documented Data Usage Requirements
5.2	Review privacy notices against regulations and business practices	<ul style="list-style-type: none"> Evaluate whether notice is required, being provided, and being tracked for each inventoried application. If a privacy notice is determined to be required and currently being provided: Conduct a legal review of the notice and policies to determine whether they meet all applicable laws and regulations. Work with business area to draft a compliant privacy notice aligned with business practices. For areas that are not operationalised, develop a plan to implement the procedures as communicated in privacy notices 	<ul style="list-style-type: none"> Documented minimum controls and requirements for data
5.3	Rationalise LSBU data	<ul style="list-style-type: none"> For each Application / process identified as storing Personal Data, consider whether data can be eliminated (per approved records retention schedules), or consolidated into a more central storage area. Require data rationalisation to reduce LSBU's overall data footprint. This could be perhaps considered in conjunction with your proposed "Identity Programme". 	<ul style="list-style-type: none"> Personal data either removed supported with evidence and justifications

6. Breach Response and Complaints Management

Having a robust management and response programme will ensure that LSBU is able to notify known issues within the required time frame of 72 hours and where personal data of data subjects is affected make the necessary external notifications to regulators, and later consumers, providing a level of trust that personal data is taken seriously.

Breach response and complaints management are techniques for risk management. It is likely that in the event of regulatory and judicial scrutiny post May 2018 organisations will be tested on their approach to these areas.

RAT results:

RAT domain	RAT question	Maturity
Challenge	Have you implemented personal data breach response procedures?	2
	Have you implemented personal data breach regulatory reporting procedures?	3
	Have you implemented assessment and notification procedures for individuals affected by a personal data breach?	4
	Do you have procedures for identifying and investigating complaints from individuals about the way their personal data is being processed?	2

Recommended work streams:

Breach Response and Compliants Management			
#	Activity	Tasks / Description	End State
6.1	Implement / strengthen personal data breach response planning	<ul style="list-style-type: none"> Perform a gap analysis of current personal data breach response procedures to the GDPR requirements. Review and update procedures covering personal data breaches including reporting to the regulator for serious breaches and reporting to the data subjects where there is a significant risk to the rights and freedoms of the data subject. Align current procedures and create a set of standardised procedures / scenarios that meet the GDPR requirements. Seek review and sign-off of standardised personal data breach response procedures. Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol to follow the prescribed GDPR format. Maintain documented process for escalation, liaison with external and internal stakeholders. 	<ul style="list-style-type: none"> Documented Breach Response and Scenario Management Procedures
6.2	Implement / strengthen Incident Management Procedures	<ul style="list-style-type: none"> Maintain a process to identify incident severity and determine required actions and escalation procedures. Maintain a log to track data privacy incidents/breaches (including facts, effects and remedial action taken as result of breach). 	<ul style="list-style-type: none"> Documented Incident Management Procedure and Logs

Breach Response and Compliants Management

6.3	Implement / Update processes relating to complaints management and response	<ul style="list-style-type: none"> • Refer to guidance in the GDPR to formally design procedures to ensure that individuals can raise issues or complaints about how their personal data is processed. • Perform a gap analysis on existing processes and whether these meet necessary requirements. • Maintain procedures to ensure each complaint is addressed, and the resolution is documented and communicated to the individual • Maintain Frequently Asked Questions to respond to queries from individuals (to be used by contact centres and HR). • Embed the procedures for allowing individuals to raise issues or complaints about how their personal data is processed into business as usual activities and communicate the new processes to the business. • Develop new policies and procedures to address data subject rights to complain or object to direct marketing 	<ul style="list-style-type: none"> • Documented Data Subject Complaints Management procedure
-----	---	---	---

7. Third Party Management

LSBU indicated that, in order to effectively comply with data protection and security requirements, there needs to be an effective management of its third parties. This can be achieved by being able to place trust in its third parties and Partners by ensuring that LSBU's personal data is processed in accordance with LSBU's data protection policy. Due to the structure of LSBU's operations, there is a large number of third parties used, especially in the international relations and student enrolment part of the University, each of whom carry their own amount of risk. Therefore an approach that is agile and able to manage risk without overcomplicating processes with third parties and Partners.

The purpose here is to ensure that LSBU has appropriate knowledge and assurance of third party processing activities of its personal data and to minimise the risk of LSBU's data being processed or shared unlawfully or without adequate safeguards.

RAT results:

RAT domain	RAT question	Maturity
Third Parties	Are third party processors assessed against their ability to meet the conditions laid out in the GDPR?	2
	Have existing third party processing contracts been updated for GDPR?	2
	Is data protection training available within third party processor organisations?	1

RAT domain	RAT question	Maturity
	Are third party processors audited for compliance with their contractual and statutory data protection obligations?	2

Recommended work streams:

Third Party Management			
#	Activity	Tasks / Description	End State
7.1	Identify all third parties and service providers who have access to or handle LSBU's personal data	<ul style="list-style-type: none"> • Prioritise third parties who have access or process LSBU personal data based on type of data held, location and amount of data held. • Assess any new supplier or third party outsource contracts to assess impact on the GDPR compliance programme. • Conduct assessments across LSBU and determine third parties who handle and have access to personal data, including student and employee data. • Assess all existing contracts / outsource agreements extending beyond May 2018, assess whether the right contractual clauses have been included to protect LSBU and personal data. • Where contracts do not contain necessary GDPR clauses, request amendments or assurances from third parties that personal data will be processed in accordance with GDPR requirements. • Risk rate third parties on basis of which pose the greatest risk to LSBU. 	<ul style="list-style-type: none"> • Register of all third parties who have access or handle personal data
7.2	Define / update a due diligence process to assess service providers / third parties security and data protection management	<ul style="list-style-type: none"> • Develop or update a third party Security and Data Protection due diligence process with input from procurement, information security, and legal. • Approve due diligence framework and implement process. • Communicate process to all employees and publish this on the central repository. • Align old and new processes. 	<ul style="list-style-type: none"> • Documented and approved third party information security due diligence
7.3	Maintain the list of third parties to keep track of all third parties who have access to or store LSBU's personal data special categories of personal data.	<ul style="list-style-type: none"> • Compile a list of all third parties identified. Use this list to support the build of the Article 30 register. • Publish list in a central repository available only to necessary stakeholders (i.e. legal, procurement, information security etc.) • Update the list with new third parties and/or when a third party has been audited, contracts have been updated, and another factors relating to the risk of the third party have changed. 	<ul style="list-style-type: none"> • Third party tracker in place
7.4	Design and implement an assurance program to monitor service providers compliance.	<ul style="list-style-type: none"> • Consult with relevant teams, including procurement, and determine and review current SLAs for identified third parties. • Develop a third party compliance programme to monitor and assess information security and Data Protection compliance of third parties, review SLA's, service credits and value for money. Compliance 	<ul style="list-style-type: none"> • Documented assurance procedure for third parties

	<p>programme should be risk based and must consider the type, amount and sensitivity data processed by third parties.</p> <ul style="list-style-type: none"> • Circulate programme with stakeholders to ensure that information security and Data Protection are addressed and KPI's are defined. • Perform regular reviews over the information security and data protection controls at third parties as per the assurance program. • Report key weaknesses / risks to the relevant data protection committee / project BAU team. • Track the progress of actions to address identified weaknesses / issues. 	
--	--	--

8. Implement DPIA and DPbD

This Data Protection Impact Assessment (“**DPIA**”) workstream is designed to identify the impact to data subjects when their personal data is processed. The DPIA will be carried out prior to any new data processing activities, new systems and solutions are implemented that handle personal data. The assessment may identify the high risks areas of processing. The DPIA may be considered as a data protection by design mechanism which will enhance data protection within LSBU by considering data protection requirements in the early stage of a programme / project.

The Data Protection by Default and Data Protection by Design (“**DPbD**”) workstream takes into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing. LSBU may implement appropriate technical and organisational measures which are designed to implement data protection principles at the beginning of a project/programme and to integrate the necessary safeguards into the processing in order to meet the GDPR requirements.

Privacy by Design, DPIAs are techniques for risk management. It is likely that in the event of regulatory and judicial scrutiny post May 2018 organisations will be tested on their approach to these areas. See again Part IV GDPR.

RAT results:

RAT domain	RAT question	Maturity
Design	Do you have policies and procedures for conducting data protection impact assessments?	2
	Do you have policies and procedures for data protection by design and by default?	2
	Are procedures in place for ensuring regulatory consultation where the output of a data protection impact assessment indicates a high level of risk for individuals?	1

Recommended work streams:

DPIA			
#	Activity	Tasks / Description	End State
8.1	Review and update data protection impact assessment framework	<ul style="list-style-type: none"> Identify the GDPR requirements for a DPIA and guidance as published by Article 29 Working Party. Build a framework to measure the impact of the DPIA outcome. Appoint accountable steering committee or accountable stakeholders to sign off the DPIAs (System owner, Business owner, DPO, etc). Update policies and procedures to reflect changes and requirements. Include DPIAs in the business change methodology, code development and, when considering EU personal data. 	<ul style="list-style-type: none"> Developed data protection impact assessment framework
8.2	Test the data protection impact assessment and Respond effectively to outcomes of DPIAs	<ul style="list-style-type: none"> Conduct a pilot DPIA in a new or existing project. Evaluate the outcome of the DPIA and its effectiveness (including resources allocation, risk identification etc.) Agree on the final DPIA framework/template. Coordinate with the GDPR compliance governance structure to ensure appropriate contact is made with regulators and individuals, in light of the results of the DPIA, if required. Implement controls to ensure DPIA results are acknowledged and resulting action items completed as required. DPIA results should be included in registers of data-related processing activities. 	<ul style="list-style-type: none"> Effective data protection impact assessment
8.3	Develop a DPbD framework	<ul style="list-style-type: none"> Decide what Data Protection by Default and what Data Protection by design means for LSBU. Build a framework and create/update policies to reflect changes. Build a training programme for DPbD (design). Make training mandatory for data architects and software engineers who are developing systems, processes or applications that handle personal data. Define KPIs to measure DPbD understanding by relevant stakeholders. 	<ul style="list-style-type: none"> Developed a DPbD framework

The associated technologies which will support DPIA and DPbD have not been included into the activities, these must not be overlooked and should be implemented once the necessary documentation and processes have been defined.

Appendix 2: LSBU Readiness Assessment Results

Appendix 2: LSBU's Readiness Assessment Results

An overview of LSBU's maturity is displayed in the tables below. The table below shows:

- **Count** - Number of questions asked for each sub-domain. E.g. 3 Governance questions were asked.
- **N/A** – Number of questions per sub-domain that not answered
- **Maturity** – The number of questions that were attributed to each maturity level.

<i>Maturity level</i>	<i>Category</i>
1	Poor
2	Developing
3	Standardised
4	Optimised

Data Protection Architecture	Count	N/A	Maturity			
			1	2	3	4
Vision and strategy	2	0	0	2	0	0
Programme build	4	1	3	0	0	0
Governance	3	0	1	2	0	0
Data protection roles and responsibility	6	0	1	5	0	0
Registers	5	0	3	2	0	0
Policies	5	0	3	2	0	0
Design	3	0	1	2	0	0
Controls	2	0	1	1	0	0
Education and awareness	1	0	0	0	1	0
Assurance	1	0	1	0	0	0
Third parties	4	0	1	3	0	0
Challenge	5	0	1	1	2	1
Accountability	2	0	0	2	0	0
Remediation	1	0	0	1	0	0
Data Protection Principles						
Lawfulness, fairness and transparency	8	0	0	7		1
Purpose limitation	2	0	2	0	0	0
Data minimisation	1	0	1	0	0	0
Accuracy	1	0	1	0	0	0
Storage limitation	2	0	2	0	0	0
Integrity and confidentiality	6	0	1	3	2	0
Rights	6	0	4	2	0	0
Transfers	2	0	0	2	0	0

Benchmarked Data

Using data taken from across our past R.A.T assessments, we are able to benchmark LSBU's existing maturity against that of other companies both in the wider population, and those specifically in the Education industry. LSBU demonstrated higher levels of maturity in some of the areas when viewed against the wider population of RAT participants (see Table 1). It should be noted that this covers all industries, some of which have a considerably lower level of reliance on technology and do not process personal data as part of the revenue producing activities.

In addition, LSBU is tracking at an average maturity with their Educational peers in some areas (see Table 2). Strengths in LSBU's roles and responsibilities, education and awareness and lawfulness, transparency and awareness suggest that this has perhaps arisen as a result of good practice being driven by the stricter regulatory scrutiny in the organisation which is supporting LSBU's efforts to become GDPR compliant.

When reviewing the benchmarking information, however, it should be noted that both the wider education sector and the population as a whole is tracking at a lower level of maturity than that required by the GDPR. An organisation that is 'GDPR ready' would be tracking at a maturity level of 3 or above across all the domains.

Table 1

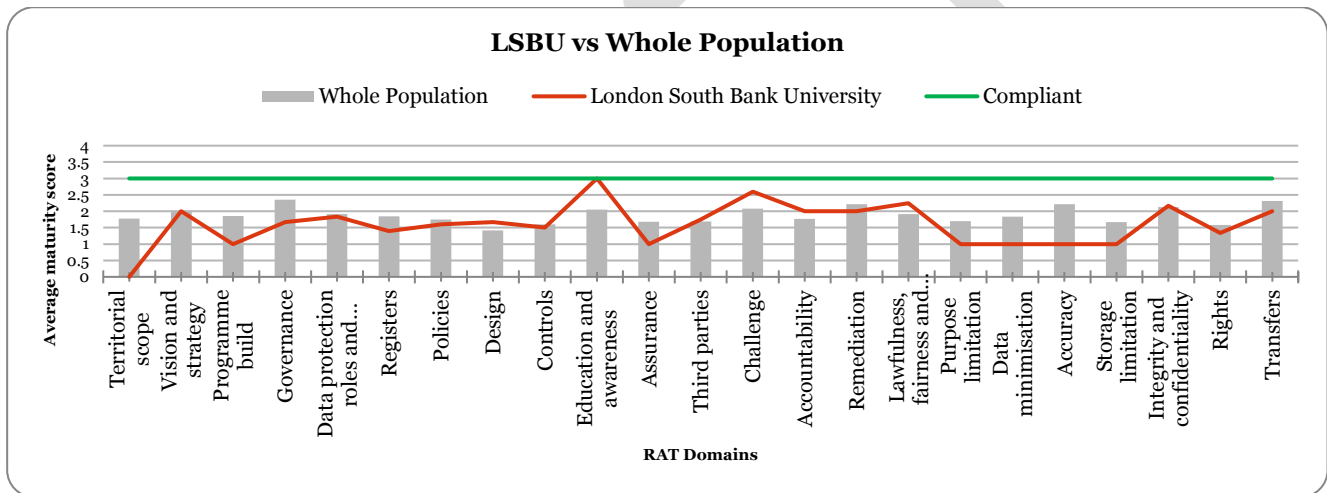
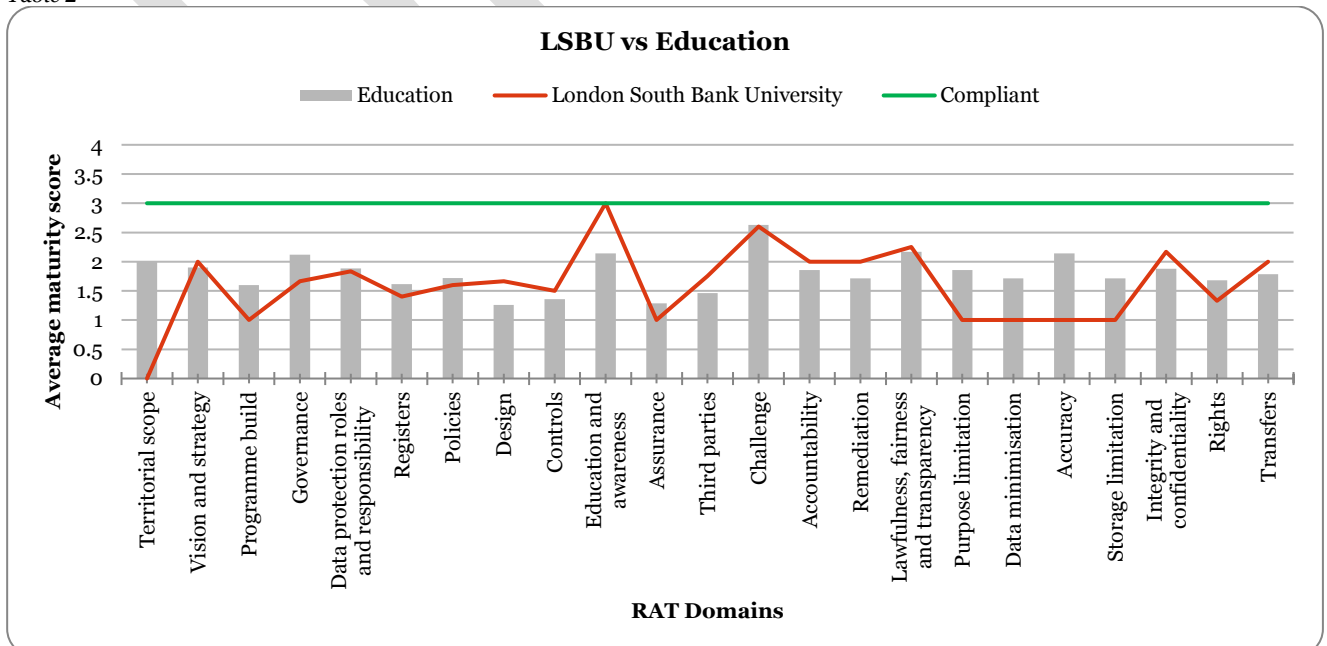


Table 2



Appendix 3: Attendee List – Special Characteristics Workshop

Appendix 3: Attendee List – Special Characteristics Workshop

Name	Role / Title
Alex Steeden	Head of Research & Insight
Andrew Casey	School Executive Administrator
Argyrios Georgopoulos	Head of Learning & Development
Craig Girvan	Head of Information Security
Ed Spacey	Head of Health Safety and Resilience
Irina Bernstein	Legal
James Pang	School Executive Administrator
James Stevenson	University Secretary
Jide Iyaniwura	Project Manager - GDPR
Joanna Killoughery	B2B Marketing Officer
Joanne Monk	Deputy Director of HR
Kathryn Gilmore	Manager, PG Admissions
Kavin Thiruchivam	Data Analyst
Michael Swire	Student Life Centre Manager
Natalie Ferer	Financial Controller
Nuria Prades	Senior International Officer
Penny Green	Head of Procurement
Rao Bhamidimarri	Vice President (Development)
Roma Sharma	Database and Compliance Manager
Scott Dunk	Manager, Strategic Recruitment & Conversion

DRAFT

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 May 2017. We accept no liability (including for negligence) to anyone else in connection with this document, and it may not be provided to anyone else.

This is a draft prepared for discussion purposes only and should not be relied upon; the contents are subject to amendment or withdrawal and our final conclusions and findings will be set out in our final deliverable.

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Annual efficiency return
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Richard Flatman
Purpose:	For approval
Recommendation:	The committee is requested to approve the report.

Executive Summary

This report asks HEFCE-funded higher education institutions to provide data on efficiencies realised in the 2016-17 academic year.

In order to report to Government on the efficiency of the HEFCE-funded higher education sector, data is collected from institutions through an annual efficiency return. Efficiency return data at the sector level will be published by HEFCE.

The annual efficiency return must be approved by the accountable officer and presented to the institution's governing body. Efficiencies data is often estimated and is not necessarily comprehensive, but institutions should provide information to the best of their knowledge.

Data is required on new efficiencies delivered in the 2016-17 academic year. Reportable efficiencies are those that release cash or resources, or result in productivity gains or capital receipts.

The report was reviewed by the Chair of the Audit Committee and submitted to HEFCE on 31 January 2018.

The Value for Money report to Audit Committee (9 November 2017) is appended for reference.

This page is intentionally left blank

Annual efficiency return for AY 2016-17

Institution: London South Bank University

UKPRN: 10004078

Declaration by Accountable Officer

I confirm that the information on efficiencies delivered in the 2016-17 academic year reported in the attached return is reasonable and has been prepared in accordance with guidance published on the HEFCE website (<http://www.hefce.ac.uk/pubs/Year/2017/201722/>).

I confirm that the governing body, or appropriate non-executive committee of the governing body, has reviewed the return.

Name of body that reviewed the return	
Date of meeting	

Where the governing body or appropriate committee is meeting after the date of this return, I confirm that the return will be reviewed at the following meeting.

Name of body that will review the return	Audit Committee
Date of meeting	08/02/18

Signature of Accountable Officer:

Name:

Title:

Date:

The name and title of the Accountable Officer must be completed before the return is uploaded to the HEFCE extranet (secure area of the HEFCE website). The results file should then be printed and signed by the Accountable Officer. Please scan the signed hard copy and upload via the HEFCE extranet.

Annual efficiency return for AY 2016-17

Institution: London South Bank University
UKPRN: 10004078

IN CONFIDENCE

To be returned no later than 31 January 2018.

Guidance for completing this return is provided on the HEFCE website:
Queries about completing this return should be directed to Matthew Davey:
Queries about the HEFCE extranet should be directed to Matthew Eagles:

<http://www.hefce.ac.uk/pubs/Year/2017/201722/>
m.davey@hefce.ac.uk
aar@hefce.ac.uk

Please provide contact details for up to two people who can respond to any questions about your return

	Contact 1	Contact 2
Name	Penny Green	Richard Duke
Position	Head of Procurement Services	Head of Planning, Performance & Assurance
Telephone Number	+44 (0)20 7815 6368	+44 (0)20 7815 6031
Email address	greenp7@lsbu.ac.uk	duker3@lsbu.ac.uk

Headline comments (4 characters remaining):

This return has been presented to LSBU's VC and Chair of Audit Committee and will go to full Audit Committee in February 17. A number of successful Value for Money (VFM) change initiatives were delivered University-wide in 1617, ranging from automation projects to free up staff time, through to service redesigns prioritising core activities. Operational expenditure, staff costs, staff time and cashable productivity gains were generated. Initiatives are reported separately by each efficiency type. Procurement outcomes are reported in the EMM (additional £2 million cashable / non cashable efficiencies). A number of initiatives have not been reported as, whilst generating VFM outcomes including improving the student experience, they could not be reported in meaningful cashable terms.

Has the Efficiency Measurement Model (EMM) survey been completed for your institution for 2016-17?:

Yes

(if yes do not report EMM efficiencies in this return - refer to guidance)

Annual efficiency return for AY 2016-17

Institution: London South Bank University
UKPRN: 10004078

Please add or remove rows as necessary. When completing the table below, please do not leave any blank rows between entries as this will cause a problem when loading into our database.

Name of activity (maximum 100 characters)	Description of activity (maximum 200 characters)	Description of expected efficiency gains (maximum 200 characters)	Area of HE	Type of efficiency	Cash value in 2016-17 of efficiency gain (compared with 2015-16) (£000)	Comments on cash value calculations (maximum 200 characters)
Increased local collaboration	Increased investment in staff time over 18 months to build local relationships led to grant bid success on mutually beneficial schemes with social value outcomes	One Off: Additional income through grant success	Estates	Additional productivity gain	1,000.0	Annualised grant value of 5 year Passmore project.
Improved Research and Enterprise systems and procedures	Increased system investment and improved internal procedures (including centralised support), led to improved bidding processes and closer collaboration with industry.	Recurrent: Additional income from more effective use of resources	Research	Additional productivity gain	750.0	Variance in Research & Enterprise bid success 1516 and 1617 including an amount offsetting additional investment in resourcing
HR System transformation	New electronic system providing core HR and payroll functionality; absence management; e-recruitment; and employee and manager self-service.	Recurrent: Staff time saved from automated processes.	Information services	Resource-releasing efficiency	461.5	Notional time saving calculations on activities costed by average staff grade. Activities include appraisal monitoring; adding starters/leavers.recruitment steps; and staff coordinating paperwork.
Growth of study abroad - short courses	Increased diversity of offer to meet customer needs, using same staffing resources and operating costs	Recurrent: Additional income from new product range	Other	Additional productivity gain	300.0	Based on 100 new FTE students at £3k each
Automation programme	Digitisation of two key processes saving staff and student time manual handling, rekeying and checking progress, resulting in an improved student experience	Recurrent: Staff time saved from digitising 'proof of student status' and 'extenuating circumstances' processes	Information services	Resource-releasing efficiency	150.0	Notional time saved by 2 FTE administrators and % of all staff time on related transactions per year
Rationalised international partnerships	Targeted approach to partnerships focussing on major partner programmes, and phasing out time spent on all non-key partnerships.	Recurrent: Staff time saved on non-key partnerships	Other	Resource-releasing efficiency	133.3	Notional time saved on 17 non-key partnerships by 5 members of staff (cost calculated by each grade).
Data warehouse asset	Dashboard reporting, consolidating multiple report sources into one system that can be analysed directly by schools and PSGs with a view to more effective student engagement and planning.	Recurrent: Staff time saved from creation of self service data dashboard reports, replacing manually assimilated reports from multiple data sources	Information services	Resource-releasing efficiency	124.0	Estimated system user time saving of 1% based on 230 users and average Unviersity salary cost of £54k
Increased internal collaboartion between People & Organisation, and Student Support	Joint approach to staff and student wellbeing reduced duplication and enabled more complex solutions to be put in place with existing resources - including multi agency safeguarding solutions.	One Off: Increased success in safeguarding bids. Match funded arrangements reduced level of University expenditure required.	Workforce	Additional productivity gain	92.0	Based on two successful collaborative bids (HEFCE catalyst funding)
Improved targeting of Library information expenditure	Improved targeting of information library expenditure reduced operating cost whilst increasing system usage (13% full text downloads, 12% serial titles and 15% increase in e-book accesses)	Recurrent: Reduced operational cost relating to system expenditure	Learning resources	Cash-releasing efficiency	87.0	Operating cost reduction between 1516 and 1617.
Consolidation of Professional Service functions	Consolidation of Interational team and Partnerships Teams to form one directorate removed need for two Director roles.	One Off: Less staff required	Other	Cash-releasing efficiency	80.0	Calculated saving from reducing staffing from two directors to one (one FTE saving with on costs)
Improved Research and Enterprise systems and procedures	Increased system investment and improved internal procedures (including centralised support) led to business growth without requiring equivalent growth levels of staff	Recurrent: Additonal staff costs avoided	Research	Cash-releasing efficiency	72.9	Calculation on additional staff required if processes had remained manual to meet the growth achieved between 15/16 and 16/17.
Student appeals process redesign	Redesign of appeals process to ensure early engagement of key staff and comprehensive standard investigation process to resolve issues and reduce number of appeals taken to formal appeal.	Recurrent: Less staff time spent overall on the end to end process as a result of less appeals progressing internally and to the OIA.	Other	Resource-releasing efficiency	59.9	2015 and 2017 variance, Case numbers multiplied by estimated resource time for each stage. Includes estimated times for key roles, costed by role's average salary.School OIA time excluded.
Improved Research and Enterprise systems and procedures	Increased system investment and improved internal procedures (including centralised support) led to reduced staff time	Recurrent: Staff time saved from automated processes, Estimated time saved by processing and completing RES forms online.	Research	Resource-releasing efficiency	57.6	Calculation based on time difference between manual and electronic process: task time by average grade of task owner, multiplied by number of electronics forms completed in 16/17.

Annual efficiency return for AY 2016-17

Institution: London South Bank University
UKPRN: 10004078

HR System transformation	New Electronic Integrated HR & Payroll system providing core HR and payroll functionality; absence management; e-recruitment; compulsory eTraining, and employee and manager self-service.	Recurrent:Operational cost savings.	Information services	Cash-releasing efficiency	53.0
Consolidation of Professional Service functions	Consolidation of Interational team and Partnerships teams removed duplication of tasks, freeing up resource time to focus on student recruitment	Recurrent:Staff time saved removing duplicated tasks	Other	Resource-releasing efficiency	43.8
Student appeals process redesign	Redesign of appeals process to ensure early engagement of key staff and comprehensive standard investigation process to resolve issues and reduce number of appeals taken to formal appeal.	Recurrent:Less operational cost relating to OIA case related fees.	Other	Cash-releasing efficiency	18.2
Lean processing of Employability Services	Streamlining of the DLHE collection survey through lean processing, digitising processes where possible.	Recurrent:Less staff required	Other	Cash-releasing efficiency	17.0
Improved Library enquiry management process	System investment with FAQ functionality, saving staff time and improving student experience	Recurrent:Staff time saved handling common enquiries	Learning resources	Resource-releasing efficiency	11.0
Extended library hours	Alternative resource model to staff cover extended library weekend opening hours out of term time avoided additional payroll costs.	Recurrent:Additional staffing costs avoided, enabling more services to be provided at almost the same cost.	Learning resources	Additional productivity gain	9.0

Print savings for all staff payslips. Recruitment advertising costs on 300 posts. Change of compulsory training provider approach from classroom to electronic.
Notional time saving of 5% multiplied across both directorates, costed by average grade.
Variance 2016 to 2017 OIA costs (cost related subscription element).
Variance in DLHE related staff cost 1516 to 1617.
Time saved on average enquiry time, multiplied by number of equires and average grade.
Calculation of staff cost difference between alternative staffing model to traditional staffing model in term time

Total recurring efficiencies (cash-releasing, resource-releasing and additional productivity gains) (£000)	3,520.2
Total one-off efficiencies (capital-receipt efficiencies) (£000)	0.0

Annual efficiency return for AY 2016-17

Institution: London South Bank University

UKPRN: 10004078

Your workbook has failed 1 validation check(s). For details please see below.

Sign-off:

1. Please ensure that you have filled in the name and title of the Accountable Officer.

Validation failed

2. The "Name of body that reviewed/will review the return" and "Date of meeting" should be completed for either a previous or future meeting, but not in both places.

Validation passed

Data:

3. Please provide the name and phone number or email address for at least one contact.

Validation passed

4. Please specify whether or not you have completed the Efficiency Measurement Model (EMM) survey for 2016-17.

Validation passed

5. There should be no blank rows between lines of data in the Data table.

Validation passed

This page is intentionally left blank

Institution name: London South Bank University

Submission from period: 2017

Q1. Please complete the following fields - the information is available from the detailed report created by the Efficiency Measurement Model.

Price Reduction:	£ 1,188,043
Added Value:	£ 737,488
Risk Reduction:	£ 0
Process Re-engineering:	£ 140,230
Sustainability:	£ 106,000
Total Gross Efficiency:	£ 2,171,761

eProcurement Transactions Details

Q2 No of purchasing Card Transactions:

Base line 2009/10:	0
Reported 2016/17:	11,072
Growth:	1,490

Q2a Value of purchasing card transactions:

Card transactions:	£ 2,064,539
--------------------	-------------

Q3: Total number of eMarketplace transactions:

Base line 2009/10:	2,096
Reported 2016/17:	1,265
Growth:	-831

Value of eMarketplace transactions:

Value:	£ 89,722
--------	----------

Are eProcurement transactions efficiencies (i.e. process efficiencies) included in the efficiency figures entered on Q1 on Gross Efficiency Details, for:

Q4. Procurement Card

Value: Yes - £67,480

Q5. eMarketplace

Value: Yes - £23,800

PMA/PCA

Q6. Has your institution completed either a PMA or PCA/PCIP in the last 4 years?

Value: Yes

Sustainability

Q7. Institutions current position on the Flexible Framework?

Comment: 3

If the Flexible Framework is not used, what other sustainable reporting do you use (eg EcoCampus or Green League table)

Comment: N/A

Collaborative procurement

Are Regional Purchasing Consortia and other consortia contract efficiencies included in the efficiencies figures entered in the response to Q1 on Gross Efficiency Details?

Value: Yes

Q8. Value of consortia efficiencies

£ 561,318

Q8a-1 Value of consortia collaborative spend

£ 16,647,532

Q8a-2 What level of spend goes through local collaborative agreements (outside of consortia collated data)

£ 0

Details of local collaborative spend

Comment: N/A

Q8b Areas of Major Spend

Please indicate for the following areas of spend the amounts included in your answer to Q1 on Gross Efficiency Details.

ICT

Efficiencies Reported:	£ 131,151
Are Regional Purchasing and other Consortia included?:	Yes

Estates

Efficiencies Reported:	£ 230,986
Are Regional Purchasing and other Consortia included?:	Yes

Library Learning Resources Centre

Efficiencies Reported:	£ 117,000
Are Regional Purchasing and other Consortia included?:	Yes

Electricity/Gas

Efficiencies Reported:	£ 14,128
Are Regional Purchasing and other Consortia included?:	Yes

Catering

Efficiencies Reported:	£ 0
Are Regional Purchasing and other Consortia included?:	No

Shared Services

Q9 Does your institution use/provide any shared services

Comment: No

EMM Verification Page

Institutional EMM efficiencies are reported net of e-procurement and consortia contract efficiencies. These are reported separately. So any e-procurement and consortia contract efficiencies you have included in the EMM figures on Gross Efficiency Details will need to be stripped out of the total gross efficiencies shown at the foot on that page. The boxes on this verification page are automatically calculated. The figures will be carried forward from the previous pages, and the total net efficiencies for your institution will be calculated automatically. You can amend these figures by editing your entries on the previous pages.

Total Gross Efficiencies

Q1. Total gross efficiencies – carried forward from Gross Efficiency: £ 2,171,761

Less

Q4. Procurement Card – carried forward from Procurement	£ 67,480
Q5. eMarketplace – carried forward from Procurement	£ 23,800
Q8. Value of Consortia efficiencies	£ 561,318
Total efficiencies to be stripped out of gross efficiencies	£ 652,598
Total Net Efficiencies are therefore	£ 1,519,164

Best Practice Indicators

Please complete field for reporting year 2016/17

Q10. Impactible Spend	£ 44,419,127
Q11. Impactible spend actively influenced by procurement function?	£ 44,419,127
Q12. Cost of procurement function?	£ 775,779
Q13. Percentage of staff in the procurement function who are Professionally qualified?	36 %
Q14. Total value of collaborative procurement through any means including local collaboration. This is automatically populated from the answers given in Q8a. To amend this figure please amend your responses in the Collaborative Spend section	£ 16,647,532
Q15. Total number of orders (N.B: not value)	16,282
Q16. Total number of electronic orders placed (N.B. inc purchasing cards)	16,282
Q17. Annual Procurement Savings (to be completed by ALL institutions)	£ 2,171,761

BPI Summary

BPI1 - Total cost of procurement function as % of impactible spend 1.75 %

BPI2 - Percentage of impactible spend channelled through collaborative procurement arrangements	37.48 %
BPI3 - Percentage of orders placed electronically and via purchasing cards	100 %
BPI4 - Percentage of impactible spend influenced by procurement function	100 %
BPI5 - Annual procurement savings as percentage of impactible	5 %
BPI6 - Percentage of qualified procurement staff	36.00 %
BPI7 - Where is the institution on the Flexible Framew	3

This page is intentionally left blank

APPENDIX – FOR BACKGROUND	
Paper title:	Value for Money update
Board/Committee	Audit Committee
Date of meeting:	9 November 2017
Author:	Penny Green, Head of Procurement
Executive/Operations sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	To Note
Recommendation:	Audit Committee is requested to note the report.

HEFCE Value for Money Reporting Requirements

To date, HEFCE, as part of its grant letter, has required HEFCE-funded institutions to produce an annual VFM report. HEFCE used information from these reports to report the aggregate efficiency of the sector. The Value for Money report was made mandatory for the first time last year, with a recommended expanded reporting scope (LSBU received positive feedback from HEFCE on our 2016 report).

HEFCE commissioned an independent review of the 15/16 VFM reports. The review analysed the nature and volume of the savings reported and the approaches taken to achieve them. It also assessed the extent to which the reports assisted governors in understanding and improving value for money, and suggested what information value for money reports should contain, based on good practice in the sector.

HEFCE issued new guidance on 6 October 2017 advising that HEFCE-funded institutions should consider reporting on value for money internally to their governing bodies, but confirming that it is no longer a requirement to submit full value for money reports to HEFCE.

New HEFCE guidance advises that under the [memorandum of assurance and accountability](#), internal auditors and audit committees are required to give an opinion, addressed to the governing body and the accountable officer, on the provider's arrangements for ensuring the three elements of value for money: economy, efficiency and effectiveness. (These reports are not new and are already provided at LSBU on an annual basis). New guidance for governors has been published 'Getting to Grips with Efficiency' that describes how governors can ensure the efficient and effective use of resources at their provider. This guide was produced by the Leadership Foundation for Higher Education, supported by funding from HEFCE.

New HEFCE Efficiency Reporting Requirements

HEFCE have introduced a new mandatory report 'Annual Efficiency Return', requiring 'HEFCE-funded higher education institutions to provide data on efficiencies realised in the 2016-17 academic year. Reportable efficiencies are those that release cash or resources, or result in productivity gains or capital receipts.

The annual efficiency return must be approved by the accountable officer and presented to the institution's governing body. The deadline for returns is Wednesday 31 January 2018.

Revised LSBU VFM/Efficiency Reporting Timetable

LSBU will continue to produce a Value for Money report for internal reporting purposes. This will be produced in January to align with the new 'Annual Efficiency' return and the Efficiency Measurement Model (EMM) returns that both have January deadlines for submission to HEFCE (NB like the VfM report, the EMM return is also not mandatory).

Given the late notification of the new requirements, HEFCE has confirmed that the Annual Efficiency return can this year be approved by Board at the earliest opportunity after submission in January.

	CONFIDENTIAL
Paper title:	Finance and Management Information (FMI) structure and leadership team
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Richard Flatman, Chief Financial Officer
Executive sponsor:	Richard Flatman, Chief Financial Officer
Purpose:	For information. To update Audit Committee regarding changes to the structure and leadership of the department and any potential succession issues.
Recommendation:	The committee is requested to note the report.

Executive Summary:

The FMI functional structure and senior leadership team charts are attached for information.

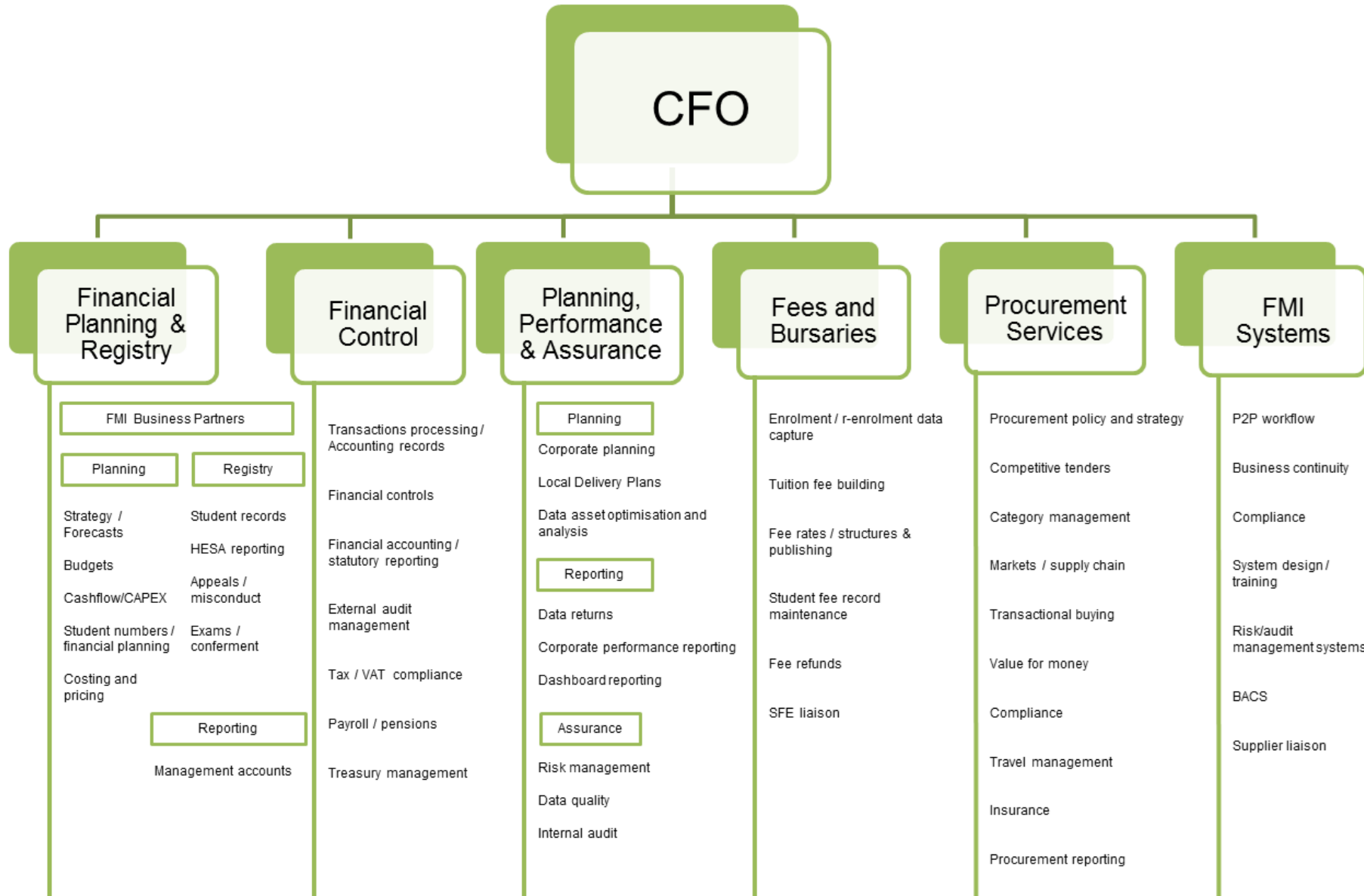
For professional services, the goal was to create a number of agile groups which, like the Schools, could develop to reflect the requirements of their customer base. Finance and Management Information (FMI) was created by combining the Finance department with elements of the Registry function. The purpose of the group is to;

- Lead the group finance function
- Facilitate the University’s business planning and corporate performance review processes through the provision of consistent financial and non-financial information
- Provide a range of assurance services covering for example risk management, value for money and data assurance, and
- Manage the internal and external audit functions

There have been no significant changes in FMI structure since the last report to Committee in February 2017.

Committee is asked to note the functional structure and leadership of FMI.

The CFO will give a verbal update at the meeting .



	CONFIDENTIAL
Paper title:	Prevent and LSBU employee update
Board/Committee:	Audit Committee
Date of meeting:	8 February 2018
Author:	Ian Mehrtens, Chief Operating Officer
Sponsor:	Ian Mehrtens, Chief Operating Officer
Purpose:	To note
Recommendation:	The Committee is requested to note the report.

1. PREVENT

- 1.1 On 27 November, the Security and Reception Services Manager was notified of a concern from a member of teaching staff in ACI concerning a possible Prevent issue.
- 1.2 A student had submitted an assignment on 26 November which included reference to *ISIS and Al Qaeda*. The student had previous mental health issues and was known to the LSBU Wellbeing Team.
- 1.3 Further background investigation within the School revealed that there had been an issue where the student had tried to make a replica gun from a 3D printer.
- 1.4 Following university procedure this issue was discussed with the Head of HR Business Services and Chief Operating Officer. It was then formally raised with the LB Southwark Prevent Officer by email on 27 November 2017. The Southwark Prevent Officer also liaised with Police and SO15 (Counter Terrorism Command).
- 1.5 It was passed by Southwark to the local authority area where the Student lives (Westminster) for action by their Prevent Advisor. A multi-agency meeting took place on 17 January 2018. Attendees included an allocated mental health nurse, and Care Leavers Team Officer (as the Student had previously been in care) plus LSBU staff.

- 1.6 At the meeting, it became clear from the nurse that the Student was also being investigated by the police for possession of live ammunition (not previously known or advised to LSBU) and police were currently testing if the replica weapon would fire ammunition.
- 1.7 A wider multi agency conference took place on 22 January 2018 at Westminster Council and as a result LSBU took the decision to suspend the student from campus with immediate effect, as discussed at the case conference.
- 1.8 Police investigations continue.
- 1.9 HEFCE was advised on 30 January 2018 and they confirmed that LSBU had followed all required actions.

2. MEMBER OF STAFF

- 2.1 A non-teaching member of staff was arrested on Monday 29 January 2018 in connection with a series of sexual assaults across south east London.
- 2.2 The member of staff appeared in court on 31 January and an application made for an extension which was granted by the court. He will appear again for a hearing on 3 February.
- 2.3 The emergency management team was mobilised and have directed the communications to staff, students, the Board and the Chancellor of the University to make sure people were informed of the facts.
- 2.4 At the time of writing, there had been limited media interest focused on LSBU and this is being monitored daily.
- 2.5 Given the serious nature of the allegations and the potential reputation risk to the University, the Vice Chancellor advised HEFCE of the incident as a “serious incident” under the Memorandum of Assurance and Accountability. HEFCE have triggered their internal PR team in case of direct approaches by the media.
- 2.6 Should there be further updates then the Board will be kept informed.

Ian Mehrtens

1st February 2018.

Paper title:	Transparent approach to costing (TRAC) return
Board/Committee	Audit committee
Date of meeting:	8 February 2018
Author:	David Kotula, Reporting Analyst
Executive/Operations sponsor:	Richard Flatman – Chief Financial Officer
Purpose:	<p>To obtain retrospective approval of the TRAC return, which is a mandatory return made to HEFCE annually in January. The purpose of the Transparency Review is to demonstrate the full costs of research and other publicly funded activities in higher education to improve the accountability for the use of public funds.</p> <p>Our return was prepared in accordance with the regulations set down by HEFCE for the preparation of the TRAC return.</p> <p>The completed return was reviewed by Ralph Sanders - Director of Planning, Information and Reporting FMI, Natalie Ferer, Financial Controller FMI, Richard Duke, Head of Performance, Planning and Assurance, and Shachi Blakemore, member of the Audit Committee.</p> <p>The report was submitted within the deadline set by HEFCE.</p>
Recommendation:	The committee is requested to approve the report.

Introduction

The Transparent Approach to Costing return (TRAC) is a mandatory return made annually in January.

The key purpose of the TRAC analysis is to provide an analysis of the costs and income allocated by Teaching, Research and Other activity.

The key risk is incorrect data analysis leading to erroneous results.

HEFCE guidance requires that the return is approved by a Committee of the Board of Governors. The purpose of this report is to provide assurance and request retrospective approval of the return for 2016/17.

Assurances regarding process

The following assurances are provided to Committee with regard to process:

1. Reconciliation to accounts

- The TRAC return is an annual return completed every January. The basis for the 2016/17 return was the financial accounts for year ending 31/07/2017. The return has been checked and reconciles to the published financial accounts
- This information includes costs down to individual staff level for teaching staff and to cost centre level for support staff. The individual staff costs are extracted from payroll data used in the Management Accounts and the staff cost data in Agresso. All figures have been reconciled back to the published accounts.

2. Compliance with guidelines/regulations

- The return has been prepared in accordance with the regulations set down by HEFCE for the preparation of the TRAC return (Ref. 2.2 – Nov 2017). This includes any updated regulations or issues raised at the TRAC self-help groups organised by the TRAC Development Group and the British Universities Finance Director's Group (BUFDG).
- Additional cost adjustments have made to the published accounts based on the Margin for Sustainability and Investment (MSI), this *replaces* the Return on Finance and Investment (RFI) and infrastructure costs adjustments. These have been calculated based on the TRAC regulations and are designed to reflect the true cost of running LSBU.
- Cost drivers are based on Time Allocation Schedules (TAS), Workload Planning datasets, student FTE derived from the HESSES16 dataset, staff FTE's derived from Payroll and HESA staff return datasets, space allocation from the EAF Tribal K2 System, and library usage data from LLR.

- All cost data is derived from the Agresso finance system at a cost centre and source code level. This data is reconciled against the source files used by the Financial Accountant to produce the published accounts.
- The robustness and accuracy of the data was verified during a review process by Ralph Sanders – Financial Planning Manager.

3 Prior Discussions and review.

- The completed return has been reviewed by Ralph Sanders - Director of Planning, Information and Reporting, Natalie Ferer, Financial Controller in her role as the data steward for Agresso, Richard Duke, Head of Performance, Planning and Assurance, and Shachi Blakemore, member of the Audit Committee.
- The final sign-off by the Vice Chancellor was on 31/01/2018.
- The report was submitted within the deadline set by HEFCE.

4 Variances.

- The 2017/18 FEC Indirect rate is £44,766 this is 2.0% lower than the prior year's figure of £45,675.
- LSBU's target surplus for sustainable operations was £16.406 million, this is now based on the Margin for Sustainability and Investment (MSI).

This page is intentionally left blank

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
UKPRN: 10004078
TRAC Peer Group: E

Declaration by Head of Institution*

I confirm that the costs, income and charge-out rate information reported in the attached return have been prepared in accordance with the TRAC requirements as set out in the TRAC guidance (Version 2.2 November 2017, <http://www.hefce.ac.uk/funding/finsustain/trac/>).

I confirm that a full self-assessment of compliance against each requirement listed in the guidance has been carried out in the last twelve months. I also confirm that a Board Committee has specifically reviewed the results of the tests for reasonableness and has either confirmed compliance or has drawn up an action plan for any areas where the institution is not fully compliant. I confirm that the Board Committee has lay membership (TRAC guidance section 2.1.5.18).

With reference to the TRAC data loaded on: 26/01/2018 10:17

Name of Board committee which confirmed compliance with the TRAC requirements.	Date of meeting at which compliance was confirmed (Please enter in the format of dd/mm/yyyy)
The Audit Committee	08/02/2018

If the Board Committee is meeting after the date of this return, please also state in the box below who provided the confirmation for this return, and the date (e.g. Chairman's Action, or management committee). Please note that responsibility still lies with the Board Committee for this confirmation.

Name of person/committee who provided confirmation for this return.	Date of confirmation (Please enter in the format of dd/mm/yyyy)
Natalie Ferer - Financial Controller	29/01/2018

Signed: (Head of Institution*) _____
 Name: David Phoenix
 Title: Chief Executive and Vice Chancellor
 Date: _____

To be returned no later than 31st January 2018. Earlier submissions are encouraged.

The name and title of the Head of Institution* must be completed before the return is uploaded to the HEFCE extranet (secure area of the HEFCE website). The results file should then be printed and signed by the Head of Institution*. Please scan the signed hard copy and upload electronically to the funding councils via the HEFCE extranet. The Funding Councils do not require a paper copy.

* Accountable Officer where this is not the Head of the Institution

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
UKPRN: 10004078
TRAC Peer Group: E

IN CONFIDENCE

To be returned no later than 31st January 2018. Earlier submissions are encouraged.

Institutional results

Data collected for use by the HE Funding Councils, Research Councils and any successor bodies

		2016-17	
		£000	As a % of expenditure
<i>Actual Operating Surplus</i>			
Total income* (derived from audited financial statements)	Calculated in Section A1	144,479	
Total expenditure* (derived from audited financial statements)	Calculated in Section A1	142,636	
Operating surplus/(deficit)		1,843	1.3%
<i>Target Operating Surplus</i>			
Target surplus for sustainable operations (EBITDA for MSI)	Calculated in Section C1	16,406	11.5%
Sustainability gap (difference between target surplus for sustainable operations and operating surplus/(deficit))			
		14,563	10.2%
Full economic cost (total expenditure + target surplus for sustainable operations)			
		159,042	111.5%

* The income and expenditure lines as reported in the Consolidated Statement of Comprehensive Income should be adjusted, where appropriate, in respect of pension costs, gains or losses on disposal of fixed assets, gains or losses on investments, the share of surpluses/deficits in joint ventures and associates, taxation charges or credits and non-controlling interests in line with section 3.1.4.8 of the TRAC guidance.

Is your institution eligible for and applying dispensation from 1 April 2018? Please select Yes/No from the drop-down box

No

(Eligibility is defined as institutions with less than £3,000,000 annual research income from public sources. A rolling average of research income (over five years) is used to assess whether £3,000,000 has been reached or not. More information on dispensation can be found in annex 1.2b of the TRAC guidance (November 2017, <http://www.hefce.ac.uk/funding/finsustain/trac/>))

Analysis of TRAC results

(A) TRAC income and full economic costs by activity

Data collected for use by the HE Funding Councils, Research Councils and any successor bodies

2016-17

	Teaching		Research £000	Other		Total £000
	Publicly funded £000	Non-publicly funded £000		Income generating activity £000	Non-commercial activity £000	
Income	106,967	9,967	6,436	20,593	516	144,479
TRAC full economic costs	115,037	9,818	13,603	20,508	76	159,042
Recovery of full economic costs (income)	93.0%	101.5%	47.3%	100.4%	675.4%	90.8%

Note: Income allocation guidance is contained in Annex 3.5a and 3.5b of the TRAC guidance and can be found here: <http://www.hefce.ac.uk/funding/finsustain/trac/>

(B) Research income and full economic costs by research sponsor type

Data collected for use by the HE Funding Councils, Research Councils and any successor bodies

2016-17

	Recurrent research funding from the funding councils								Total Research £000
	£000	Institution-own funded £000	Postgraduate research £000	Research Councils £000	Other govt departments £000	European Union ¹ £000	UK-based Charities £000	Industry ² £000	
Income	1,771	314	1,262	657	571	1,092	260	509	6,436
TRAC full economic costs		953	8,357	822	713	1,731	350	677	13,603
Recovery of full economic costs (income)		32.9%	15.1%	79.9%	80.1%	63.1%	74.3%	75.2%	47.3%

¹ European Union covers EU government bodies including the Commission. This is the same as that defined under 3(h) in Table 7 of the HESA Finance record.

² Industry should include all other organisations such as UK industry, commerce and public corporations, UK Other, EU non-government organisations (i.e. EU-based charities, EU industry and EU other) and Overseas organisations (Non-EU based charities, Non-EU industry and Non-EU other).

For further details of definitions please see sections 3.1.4.1 and 1.3.2 of the TRAC guidance (<http://www.hefce.ac.uk/funding/finsustain/trac/>).

It is not currently a TRAC requirement to reallocate income and costs relating to PGR activity away from the external research sponsor type to the PGR category. However it is possible this could become mandatory, at least for research intensive institutions in the future. Please indicate in the box on the right whether your institution already reallocates income and costs to the PGR category. If you do not have any PGR income or costs please select "N/A".

No, we do not reallocate income and costs away from the external research sponsor type to the PGR category.

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

IN CONFIDENCE

Further analysis of TRAC results

(A1) Derivation of TRAC income and expenditure figures

Data collected for use by the HE Funding Councils and any successor bodies

	2016-17 £000
Total income ¹	144,479
+ gain on disposal of fixed assets	0
+ gain on investments	
+ share of operating surplus in joint ventures	0
+ share of operating surplus in associates	0
+ taxation credit	0
TRAC income	144,479
Total expenditure ²	142,636
minus cost or plus credit attributable to the periodic revaluation of [USS and SAUL] pension scheme liabilities	0
+ [USS and SAUL] employer pension deficit contributions excluded from expenditure in financial statements	0
+ loss on disposal of fixed assets	0
+ loss on investments	0
+ share of operating deficit in joint ventures	0
+ share of operating deficit in associates	0
+ taxation charges ³	0
plus surplus or minus deficit attributable to non-controlling interests	0
TRAC expenditure	142,636

¹ From FRS 102 accounts - income as reported in the Consolidated Statement of Comprehensive Income

² From FRS 102 accounts - expenditure as reported in the Consolidated Statement of Comprehensive Income

³ Taxation charges should include all charges reported in the Consolidated Statement of Comprehensive Income, including taxation on research and development expenditure credit (RDEC)

(A2) TRAC income and full economic costs by activity - Further analysis

Please select which model has been applied to account for government grants:

Government revenue grants Accrual model
 Government capital grants (excluding grants for land) Accrual model

	Teaching		Research	Other		Total
	Publicly funded £000	Non-publicly funded £000		Income generating activity £000	Non-commercial activity £000	
Items included in income						
TRAC income	106,967	9,967	6,436	20,593	516	144,479
Donations and Endowments (note 1)						
New Endowments received and included in total income	0	0	0	0	0	0
New Donations included in total income	0	0	0	0	0	0
New capital grants received in the year (note 2)						
New Government Capital Grants included in total income	0	0	0	0	0	0
New Non Government Capital Grants included in total income	0	0	0	0	0	0
Material (Exceptional) income (note 3)						
Other material items (included in total income)***	0	0	0	0	0	0
Total income after adjusting for the above items	106,967	9,967	6,436	20,593	516	144,479
Items included in full economic costs						
TRAC full economic costs (from Section A)	115,037	9,818	13,603	20,508	76	159,042
Material (Exceptional) expenditure (note 3)						
Staff restructuring costs (included in total expenditure)	606	0	0	0	0	606
Costs of fundamental reorganisation or restructuring (included in total expenditure)	0	0	0	0	0	0
(Gain) or loss on sale or termination of an operation (included in total income or total expenditure as appropriate)	0	0	0	0	0	0
Other material items (included in total expenditure)***	0	0	0	0	0	0
Total full economic costs after adjusting for the above items	114,431	9,818	13,603	20,508	76	158,436

***To include where separately analysed on the face of the Consolidated Statement of Comprehensive Income

Note: Income allocation guidance is contained in Annex 3.5a and 3.5b of the TRAC guidance and can be found here: <http://www.hefce.ac.uk/funding/finsustain/trac/>

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

(B1) Research income and full economic costs by research sponsor type - Further analysis

2016-17	Recurrent research funding from the funding councils £000	Institution-own funded £000	Postgraduate research £000	Research Councils £000	Other govt departments £000	European Union* £000	UK-based Charities £000	Industry** £000	Total Research £000
Items included in income									
TRAC income	1,771	314	1,262	657	571	1,092	260	509	6,436
<i>Donations and Endowments (note 1)</i>									
New Endowments received and included in total income	0	0	0	0	0	0	0	0	0
New Donations included in total income	0	0	0	0	0	0	0	0	0
<i>New capital grants received in the year (note 2)</i>									
New Government Capital Grants included in total income	0	0	0	0	0	0	0	0	0
New Non Government Capital Grants included in total income	0	0	0	0	0	0	0	0	0
<i>Material (Exceptional) income (note 3)</i>									
Other material items (included in total income)***	0	0	0	0	0	0	0	0	0
Total income after adjusting for the above items	1,771	314	1,262	657	571	1,092	260	509	6,436
Items included in full economic costs									
TRAC full economic costs (from Section A)		953	8,357	822	713	1,731	350	677	13,603
<i>Material (Exceptional) expenditure (note 3)</i>									
Staff restructuring costs (included in total expenditure)		0	0	0	0	0	0	0	0
Costs of fundamental reorganisation or restructuring (included in total expenditure)		0	0	0	0	0	0	0	0
(Gain) or loss on sale or termination of an operation (included in total income or total expenditure as appropriate)		0	0	0	0	0	0	0	0
Other material items (included in total expenditure)***		0	0	0	0	0	0	0	0
Total full economic costs after adjusting for the above items		953	8,357	822	713	1,731	350	677	13,603

***To include where separately analysed on the face of the Consolidated Statement of Comprehensive Income

Notes for A2 and B1:

- Both unrestricted donations and restricted donations (endowments) are typically recorded in income when received and form part of the TRAC data income in the year the income is received (associated expenditure is recorded in the year it is made).
- The total income figure reported in the consolidated financial statements will include income from capital grants as well as from revenue grants. If the accrual model is adopted for government capital grants, on recognition the capital grant element will be shown as deferred income and then released as funding body, research or other income as appropriate; whereas if the performance model is adopted for government capital grants the capital grant will be recognised as funding body, research, or other income, as appropriate, when performance conditions are met. The total income figure reported under TRAC does not adjust the total income figure reported in the consolidated financial statements for the government capital grant accounting policy adopted by the institution. There is no such accounting policy choice for non-government capital grants which are recognised as income when performance conditions are met.
- Exceptional items are not defined by FRS 102. Under FRS 102 items previously classified as exceptional items (as defined by FRS 3 in previous UKGAAP) are known as material items and are included in the main income and expenditure headings. Such items should be included in TRAC income or cost but may be separately analysed in the Annual TRAC return other than those previously analysed "below the line": fundamental restructuring costs and losses on sale or termination of an operation.

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

IN CONFIDENCE

(C) Calculation of the Margin for Sustainability and Investment

Data collected for use by the HE Funding Councils, Research Councils and any successor bodies

The MSI is given by the institution's average required level of cash generation (EBITDA) over six years, divided by the adjusted income for the current year. All numbers used in the table below should be taken from either the audited financial statements or the financial forecast as approved by your Governing Body.

C.1 Adjusted Earnings Before Interest, Tax, Depreciation and Amortisation (EBITDA) for MSI

	Actual 2014-15 £000	Actual 2015-16 £000	Actual 2016-17 £000	Forecast 2017-18 £000	Forecast 2018-19 £000	Forecast 2019-20 £000	6 year average £000	
Surplus/(deficit) ¹	-1,172	3,270	1,842	1,500	2,200	4,000	1,940	Enter surpluses as positive values and deficits as negative values
Share of surplus/(deficit) in joint venture(s) and associates	0	0	0	0	0	0	0	Enter surpluses as positive values and deficits as negative values
Finance charges ²	4,724	4,755	4,369	4,408	4,408	4,408	4,512	Enter as a positive value
Depreciation	8,759	9,749	9,620	11,130	11,256	11,714	10,371	Enter as a positive value
Amortisation (including impairment charges)	0	0	0	0	0	0	0	Enter as a positive value
Capital grants received/receivable (for non-government capital grants and for government capital grants where the performance model is adopted) ³	0	0	0	0	0	0	0	Enter as a negative value
Release of deferred capital grants from all sources (accruals model only)	0	-1,379	-1,126	0	0	0	-418	Enter as a negative value
New permanent endowments	0	0	0	0	0	0	0	Enter as a negative value
Staff charges/(credits) arising from pension provisions (including both self-administered trust defined benefit schemes and deficit recovery provisions on multi-employer schemes)	0	0	0	0	0	0	0	Enter charges as a positive value and credits as a negative value
Fair value changes to financial instruments (where hedge accounting policy choice is NOT applied)	0	0	0	0	0	0	0	Enter gains as a negative value and reductions as a positive value
EBITDA for MSI	12,311	16,395	14,705	17,038	17,864	20,122	16,406	

¹ This should be taken from the statement of comprehensive income and is the surplus/(deficit) before other gains/losses and share of surplus/(deficit) in joint ventures and associates. Gross RDEC income should be deducted from the surplus/(deficit).

² This should include interest payable on debt, finance leases and service concessions, pension deficits and the unwinder of discount rates with respect to the valuation of provisions (eg. provisions for multi-employer pension schemes).

³ Capital grants taken to income (for all non government capital grants, and government capital grants where the performance model is adopted) (please enter as negative)

C.2 Margin for Sustainability and Investment (MSI)

	£000
Total income (per audited financial statements 2016-17)	144,479
Release of deferred capital grants 2016-17 (accrual model only)	-1,126
Capital grants included in income 2016-17	0
New permanent endowments 2016-17 ⁴	0
Adjusted total income 2016-17	143,353
MSI	11.4%

RDEC income as reported in the 2016-17 HESA Finance Record (£000s)

Gross RDEC income	RDEC taxation	Net RDEC income
0	0	0

⁴ New permanent endowments included in income should be deducted. New expendable endowments or other donations should not be adjusted for here

C.3 Apportionment of the 'EBITDA for MSI' between TRAC categories

The MSI should be allocated between the TRAC categories (T, R and O) on the basis of apportionment of TRAC expenditure between T, R and O.

	Teaching	Research	Other	Total
TRAC expenditure (£000s)	110,934	12,641	19,061	142,636
EBITDA for MSI (£000s)	12,759	1,454	2,192	16,406

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

(D) Calculation of indirect and estates cost charge-out rates for Research

Data collected for use by the Research Councils and any successor bodies

Please select box (shown on the right) if you do not calculate an estates laboratory rate or an estates non-laboratory ra

2016-17 charge-out rate indexed two years

			Indirect	Estates non-laboratory	Estates laboratory
Cost per TRAC allocated to research ¹			6,302	345	1,243
Academic staff	FTEs	(i)	624.3	149.8	474.5
% research time of academic staff		(ii)	10.1%	10.1%	10.1%
Resulting in direct time of academic staff		(i) * (ii)	63.1	15.1	47.9
Research assistants and fellows	FTEs		38.0	11.0	27.0
PGRs	FTEs		219.4	102.0	117.4
	weighted by		0.2	0.5	0.8
	weighted FTEs		43.9	51.0	93.9
Total FTEs			144.9	77.1	168.8
Rate (£)			43,482	4,473	7,362
Indexation (two years) %			3.0%	3.0%	3.0%
Indexed year 1 rate (£)			44,786	4,607	7,583

¹ Indirect cost pools should include staff restructuring costs other than the costs of a fundamental reorganisation or restructuring. See TRAC guidance 3.2.5.7. The laboratory estates costs should exclude all costs of laboratory technicians and research facilities (which are reported under E.1 below). The non-laboratory estates costs should include relevant elements of these costs, unless you are charging them separately (when again they would then be reported under E.1). The cost in the numerator of the Research indirect cost charge-out rate should be reduced by any income received from the Apprenticeship Service Account for research staff (see TRAC guidance 4.2.4.3).

Do you calculate and apply different indirect rates for each department? Please select Yes/No from the drop-down box No
 If Yes please list the departments and the rates in table D(a) in the worksheet "RCUK_Departmental_rates"

Do you calculate and apply different estates rates for each department? Please select Yes/No from the drop-down box No
 If Yes please list the departments and the rates in table D(a) in the worksheet "RCUK_Departmental_rates"

(E) Calculation of laboratory technician and research facility charge-out rates for Research

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

Data collected for use by the Research Councils and any successor bodies

In section E, it is not a TRAC requirement to identify laboratory technician costs in non-laboratory departments separately from estates costs. If you do identify laboratory technician costs separately, please respond using the drop-down box (this will provide you with cells to enter data in the tables below).

Please choose an option from the drop-down box to inform us if you have no lab technicians and/or no research facilities No research facilities

	Research		Total £000
	Non-laboratory ¹ £000	Laboratory £000	
E.1 Total costs allocated to Research			
1. Research facilities ²			
2. Laboratory technicians			
a. DI ³		0	0
b. Pool		150	150
c. Infrastructure		0	0
Total		150	150
Total costs		150	150

Note:
¹ Many institutions will not have identified these costs separately from estates costs in non-laboratory research disciplines. It is not a TRAC requirement.
² The row titled Research facilities should include all costs included in the calculations of the charge-out rates for research facilities, whether charged as DI or DA.
³ Please enter the costs of all DI technicians allocated to research irrespective of whether their salary was allocated wholly to DI, or partly to Support and partly to DI.

Please describe the rates that you calculate and apply on research facilities on table E(a) in the worksheet "RCUK_Departmental_rates"

Annual TRAC return reporting for AY 2016-17

Institution: London South Bank University
 UKPRN: 10004078
 TRAC Peer Group: E

E.2 Analysis of total estates costs allocated to Research (this table will automatically be completed with information from sections D and E.1.)	Non-		Total £000
	laboratory ¹ £000	Laboratory £000	
1. Estates costs included in the estates cost rate calculation	345	1,243	1,588
2. Gross estates costs (i.e. estates plus all technicians and all research facilities.)	345	1,393	1,738
3. % of gross estates costs			
a. Research facilities			
b. Laboratory technicians			
i. DI		0.0%	0.0%
ii. Pool		10.8%	8.6%
iii. Infrastructure		0.0%	0.0%
Total		10.8%	8.6%
Total	0.0%	10.8%	8.6%

Note - It is assumed here, for benchmarking purposes only, that all research facility and laboratory technician costs were originally part of a gross estates cost (even though in practice some of these costs would have been DI and not in the estates cost total at all and some of these costs may have been in indirect costs). The gross estates cost is calculated for you on row E.2.2. No research facility or laboratory technician cost (whether DI or DA) are in the estates cost total that is used for the estates cost rate calculation - row E.2.1.

E.3 Calculation of laboratory technician infrastructure rate

2016-17 charge-out rate indexed two years

	Non-		Total
	laboratory ¹	Laboratory	
Total laboratory technician infrastructure costs (£000)		0	0
Academic/researcher/PGR FTEs		0.0	0.0
Laboratory technician infrastructure rate per FTE (£)		0	0
Indexation (Two years) %		0.0%	0.0%
Indexed year 1 rate (£)		0	0

Do you calculate and apply laboratory technician infrastructure rates separately for each department

No

If Yes please list the departments and the rates in table D(a) in the worksheet "RCUK_Departmental_rates"

(F) Analysis

Data collected for use by the Research Councils and any successor bodies

F.1 Analysis of Support costs

Estates costs and indirect costs

	Teaching £000	Research £000	Other - academic department activities £000	Other - standalone enterprise activities such as residences, catering and (most) trading companies ¹ £000	Total £000
Estates costs					
Estates costs (excluding research facilities and lab technicians)	3,423	238	700	0	4,361
EBITDA for MSI	16,203	1,350	411	3,821	21,785
Indirect costs ²					
Support time of academic staff	14,501	1,478	354	0	16,333
Central services	57,201	3,698	249	0	61,148
Support staff in academic departments	1,603	705	93	0	2,401
Non-staff costs in academic departments	0	0	0	0	0
EBITDA for MSI	3,985	421	501	0	4,907
Total indirect costs	77,290	6,302	1,197	0	84,789
Total Estates and Indirect costs	96,916	7,890	2,308	3,821	110,935

¹ Please refer to section 1.3.3 of the TRAC guidance (<http://www.hefce.ac.uk/funding/finsustain/trac>)

² Indirect cost pools should include staff restructuring costs other than the costs of a fundamental reorganisation or restructuring. See TRAC guidance 3.2.5.7. The indirect cost pool should also be reduced by any income received from the Apprenticeship Service Account for research staff (see TRAC guidance 4.2.4.3).

F.2 Analysis of staff time

Number of academic and research staff in the year (FTEs)

Academic staff covered by Time Allocation Survey ³	624.3
Research assistants & fellows (wholly charged to R)	38.0
Other academic staff (wholly charged to T or O)	36.0
Total academic and research staff FTEs	698.3

³ Academic staff covered by the time allocation survey reported in the table above should be the total number of academic staff who are covered by the current AST percentages, irrespective of whether they provided time estimates this year or in either of the two prior years, or whether they were actually part of the sample selected to provide data or not.

Academic staff covered by Time Allocation Surveys for the whole institution

	Teaching	Research	Other	Support	Total
% time unweighted for salaries ⁴	74.0%	8.2%	2.8%	15.0%	100.0%
% time weighted for salaries	65.2%	10.1%	1.9%	22.8%	100.0%
Academic staff costs (£000s)	23,411	3,621	967	16,333	44,332

⁴ See section 4.2.4.4 of the TRAC guidance (<http://www.hefce.ac.uk/funding/finsustain/trac>).

This table shows the institutional total of the department percentages that have been used to allocate academic staff costs.

Support for Teaching, Support for Research, Support for Other should all be shown under Support.

Annual TRAC return reporting for AY 2016-17

Your workbook has passed all validation checks

Please provide contact details for up to two people who can respond to any questions about your return		
	Contact one	Contact two
Name	David Kotula	
Position	Reporting Analyst	
Telephone Number	0207 815 6361	
Email address	kotulad@lsbu.ac.uk	

To improve communications with those responsible for the governance of the TRAC process please provide the name and contact details for the chair of your TRAC oversight group

Name	
Position	
Telephone Number	
Email address	

Checklist
Validation passed

Please ensure all aspects of the TRAC return have been completed in accordance with this checklist.
 Select Yes, No or N/A from the drop-down boxes

1. Has your institution used version 2.2 of the TRAC guidance published in November 2017 (http://www.hefce.ac.uk/funding/finsustain/trac) in the preparation of this return and read the change log at Annex 1.1a?	Yes
2. Do academic and research assistant/fellow staff numbers reconcile with those used as cost drivers?	Yes
3. Do PGR numbers reconcile with those included in student number cost drivers?	Yes
4. Have research facility and laboratory technician costs been allocated to Teaching and Other activities where appropriate and excluded from the research facility or laboratory technician rates?	Yes
5. Have PGR scholarships, bursaries etc been excluded from the indirect costs for Research?	Yes
6. Have Teaching costs been taken into the TRAC (T) model? (select N/A if you are an institution in Wales)	Yes
7. Are total income and total expenditure (reported in section A1) consistent with the data reported in the financial statements and the HESA finance record?	Yes
8. Has a Board Committee confirmed the results have been prepared in accordance with the TRAC requirements based on a full self-assessment of compliance (TRAC guidance section 2.1.4.3, http://www.hefce.ac.uk/funding/finsustain/trac)?	Yes
9. Do you currently use TRAC data for internal management purposes? If so, please provide examples in the comment box at the end of the checklist section.	Yes
10. Does your institution use a workload planning/management approach to time allocation data (see section 3.1.4.26 of the TRAC guidance, http://www.hefce.ac.uk/funding/finsustain/trac)?	Yes
11. Do you consider that your time allocation data and TRAC cost data are robust and provide utility to your institution?	Yes
12. Has the MSI been calculated in accordance with the guidance provided at section 3.2 of the TRAC guidance (http://www.hefce.ac.uk/funding/finsustain/trac)?	Yes

Comment box to provide examples of internal uses of TRAC data.

We use TRAC data for Space Usage utilisation analysis.

Please type directly into this comment box, rather than copying and pasting text. Pasting text may cause errors when you upload your return.

Commentary Section

Please upload an electronic commentary document along with your completed return to explain any of the following (if highlighted in purple):

Commentary documents should be submitted as a Word or PDF document via the secure area of the HEFCE website (HEFCE extranet)

- Recovery of full economic costs on PFT is more than 105%.
- Recovery of full economic costs on NPFT is less than 100%.
- Recovery of Other -Income generating activity is less than 100%
- Recovery of Other -Non-commercial activity is less than 100%
- Recovery of full economic costs on industry activity is less than 75%.
- Recovery of full economic costs on Research Councils activity is less than 30% or more than 80%.
- Recovery of full economic costs on Research Council activity is less than the recovery of full economic costs on charities activity.
- Recovery of full economic costs on Research Council activity is less than the recovery of full economic costs on European Union activity.
- Recovery of full economic costs on Other Government Department activity is less than recovery of full economic costs on Research Council activity.
- Recovery of full economic costs on Research Council activity, Charities activity, European Union activity and/or Other Government Department activity is more than 100%.
- MSI is less than 5.0% or greater than 15.7%.

¹ The Industry should include all other organisations such as UK industry, commerce and public corporations, UK Other, EU non-government organisations (i.e. EU-based charities, EU industry and EU other) and Overseas organisations (Non-EU based charities, Non-EU industry and Non-EU other).

Annual TRAC return reporting for AY 2016-17

Your workbook has passed all validation checks

Workbook validation checks

Please review the validation failures/warnings below to ensure that your data have been completed correctly before submitting your return to HEFCE. If you have a genuine reason for a validation failure/warning, please provide a brief explanation in the box at the bottom of this page. Further detail can be provided in your commentary document if required.

Commentary documents should be submitted as a Word or PDF document via the HEFCE extranet.

Declaration

1. The name of a Board Committee and a date of the meeting at which compliance with the TRAC requirements was confirmed should be entered in the "Signoff_Sheet" worksheet.

Validation passed

2. The name and title of the Head of Institution should be entered on the "Signoff_Sheet" worksheet.

Validation passed

Institutional Results

3. Only those institutions who have selected that they are not eligible for or applying dispensation should complete section D, E and F.

Validation passed

4. EBITDA for MSI would usually be greater than zero.

Validation passed

5. The question on whether your institution is eligible for and applying dispensation should be completed.

Validation passed

Section A

6. Total income recorded in section A should equal total income recorded in the institutional results section for each year.

Validation passed

7. Total full economic costs recorded in section A should equal the full economic cost recorded in the institutional results section for each year.

Validation passed

8. Both categories of 'Other' activities should be completed.

Other: Income-generating Validation passed

Other: Non-commercial Validation passed

Confirm

Confirm

Section A2

9. Please enter information on which model has been applied to account for government grants

Validation passed

10. Please ensure you have completed Table A2.

Validation passed

Section B

11. Recurrent research funding from the funding council should be recorded in the income line of the first column in section B, and should reconcile to the funding you were allocated.

Validation passed

Comment box to explain discrepancies.

Empty comment box for discrepancies.

12. Total research income recorded in section B should equal total research income recorded in section A.

Validation passed

13. Total research costs recorded in section B should equal total research costs recorded in section A.

Validation passed

14. The question on the reallocation of income and costs relating to PGR activity away from the external research sponsor type should be completed.

Validation passed

Section B1

15. Total research income recorded in section B1 should equal total research income recorded in section A2.

Validation passed

16. Total research costs recorded in section B1 should equal total research costs recorded in section A2.

Validation passed

17. If the "Accrual model" has been selected for government capital grants then 'New Government Capital Grants included in total income' in Tables A2 and B1 should be zero. Please put in a comment below to explain any discrepancies.

Validation passed

Comment box:

Empty comment box for discrepancies.

18. Please ensure you have completed Table B1.

Confirmation provided if you have no figures to enter into Table B1, please select 'Confirm'.

Confirm

Section C

19. All years of data (actual and forecast) should be completed in Table C1.

Validation passed

20. The total TRAC expenditure in Table C3 should be equal to the TRAC expenditure recorded in the institutional results section.

Validation passed

21. If the "Performance model" has been selected for the model applied to account for Government capital grants in Table A2, then the 'Release of deferred capital grants from all sources (accruals model only)' in Table C1 would usually be zero.

Validation passed

22. If there are new government capital grants in Table A2 and B1, then the 'Release of deferred capital grants from all sources (accruals model only)' in Table C1 would usually be zero.

Validation passed

Annual TRAC return reporting for AY 2016-17

Your workbook has passed all validation checks

Section D

23. If you have identified that you do not calculate an estates laboratory rate or an estates non-laboratory rate in the drop-down box in section D, then the relevant columns should be left blank.

Validation passed

24. Academic staff numbers allocated to estates should be equal to or within 10% of those allocated to indirect costs.

Validation passed

25. The % research time of academic staff (any column in row ii) would usually be less than 50%.

Validation passed

26. The % research time of academic staff in the indirect column should not be greater than both of the % research time returned in the two estates columns or less than both of the % research time returned in the two estates columns.

Validation passed

27. Direct time of academic staff in estates should be equal to or within 10% of those allocated to indirect costs.

Validation passed

28. If academic staff numbers (estates) equals indirect staff numbers (row (i)), then the direct time of academic staff (indirect) should equal the direct time of academic staff in the estates columns (row (i) * (ii)).

Validation passed

29. Research assistant/fellows numbers allocated to estates should be equal to or within 10% of those allocated to indirect costs.

Validation passed

30. PGR student numbers allocated to estates should be equal to or within 10% of those allocated to indirect costs.

Validation passed

31. Indexation should not be negative or 0 and would usually be less than 10%.

Validation passed

Section E

32. If you do not identify laboratory technician costs in non-laboratory departments (i.e. you have left the first drop-down box at the top of section E blank), then the relevant column in all of section E should be left blank.

Validation passed

33. Please ensure you have recorded whether you have lab technicians and/or research facilities consistently in table E.1. and the second drop-down box at the top of section E.

Validation passed

34. Institutions recording laboratory estates costs in section D should identify some laboratory costs in table E.1.

Validation passed

35. Laboratory technician infrastructure rate per FTE (£) in table E.3 should be completed.

Validation passed

36. Academic/researcher/PGR FTEs in table E.3 should be equal to the total FTEs in section D (for both laboratory and non-laboratory columns).

Validation passed

37. Research-intensive institutions (those in TRAC peer groups A or B) would usually report laboratory technician infrastructure rates in table E.3.

Validation passed

38. Research-intensive institutions (those in TRAC peer groups A or B) would usually report research facilities in table E.1.

Validation passed

39. If you calculate a laboratory technician infrastructure rate, please enter an indexed rate i.e. indexation should not be negative or 0 and would usually be less than 10%.

Validation passed

Section F

40. Research Indirect costs in table F.1 should equal those recorded in the first line of section D

Validation passed

41. Research estates costs in table F.1 should equal those recorded in the first line of section D.

Validation passed

42. Total support time for academic staff from table F.1 should be equal to the academic staff costs for support reported in table F.2.

Validation passed

43. Academic staff FTEs allocated to indirect costs in section D should be within 10% of Academic staff covered by Time Allocation Survey in table F.2

Validation passed

44. Research assistants and fellows in table F.2 should equal those in section D.

Validation passed

45. Percentage time unweighted for salaries for research in table F.2 should be equal to the percentage research time for academic staff recorded in section D.

Validation passed

46. Percentage time weighted for salaries should be completed in table F.2.

Validation passed

47. The total % time of academic staff (both weighted and unweighted for salaries) in table F.2 should equal 100%

Validation passed

48. Please check that costs in table F.1 have been correctly split between 'Other - academic department activities' and 'Other - standalone enterprise activities such as residences, catering and (most) trading companies'.

Validation passed

Confirm

Other

49. Contact details for at least one person who can respond to any questions regarding your return should be entered in the box at the top of this page.

Validation passed

50. Monetary values in the workbook should be entered in pounds thousands (£000).

Validation passed

Annual TRAC return reporting for AY 2016-17

Your workbook has passed all validation checks

Post submission Validation Section

Data will be subject to some additional validation checks on submitting the data to HEFCE. The results of these will appear below in the results package.

If, for any reason, you get any validation failures/warnings, you should review your figures to ensure they have been completed correctly. If this is a data error then please correct your figures in the annual TRAC return and resubmit your workbook to HEFCE.

51. Total income reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

52. Total expenditure reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

53. The net of gains and losses on disposal of fixed assets reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

54. The net of gains and losses on investments reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

55. The net of surpluses and deficits in joint venture(s) reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

56. The net of surpluses and deficits in associates reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

57. The net of taxation credits and taxation charges reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

58. The surplus/deficit attributable to non-controlling interests reported in the Annual TRAC return (Section A1) should be consistent with data in table 1 of the HESA Finance record returned in December 2017.

Validation passed

If you have a genuine reason for failing any of the above validation checks, please enter a brief explanation of this in the table below.

Validation check	Reason for failure

	STRICTLY CONFIDENTIAL
Paper title:	Committee business plan, 2017/18
Board/Committee	Audit Committee
Date of meeting:	8 February 2018
Author:	Joe Kelly, Governance Officer
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

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.

The Audit Committee is requested to note its annual business plan.

This page is intentionally left blank

Audit committee business plan, 2017/18

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
3 October 2017					
Internal audit charter			Audit Committee	3 Oct 2017	Richard Flatman
Public benefit statement			Audit Committee	3 Oct 2017	James Stevenson
Corporate governance statement			Audit Committee	3 Oct 2017	James Stevenson
Corporate Risk register			Audit Committee	3 Oct 2017	Richard Flatman
Speak up report			Audit Committee	3 Oct 2017	James Stevenson
Pensions assumptions			Audit Committee	3 Oct 2017	Richard Flatman
Membership and terms of reference			Audit Committee	3 Oct 2017	Michael Broadway
Internal controls - annual review of effectiveness	Executive	27 Sep 2017	Audit Committee	3 Oct 2017	Richard Flatman
Internal audit progress report	Executive	27 Sep 2017	Audit Committee	3 Oct 2017	Richard Flatman

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
Draft internal audit annual report	Executive	27 Sep 2017	Audit Committee	3 Oct 2017	Richard Flatman
Audit Committee business plan			Audit Committee	3 Oct 2017	Michael Broadway
Anti-fraud, bribery and corruption report			Audit Committee	3 Oct 2017	Richard Flatman
Risk strategy and appetite	Executive Audit Committee	27 Sep 2017 3 Oct 2017	Board of Governors	12 Oct 2017	Richard Flatman
10 November 2017					
Corporate risk register	Operations Board	17 Oct 2017	Audit Committee	9 Nov 2017	Richard Flatman
Speak up report			Audit Committee	9 Nov 2017	James Stevenson
Internal audit progress report	Executive	25 Oct 2017	Audit Committee	9 Nov 2017	Richard Flatman
Final internal audit annual report			Audit Committee	9 Nov 2017	Richard Flatman
External audit performance against KPIs			Audit Committee	9 Nov 2017	Richard Flatman

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
External audit - review of non-audit services			Audit Committee	9 Nov 2017	Michael Broadway
Audit Committee business plan			Audit Committee	9 Nov 2017	Michael Broadway
Audit Committee annual report	Executive	25 Oct 2017	Audit Committee	9 Nov 2017	James Stevenson
Anti-fraud, bribery and corruption report	Executive	25 Oct 2017	Audit Committee	9 Nov 2017	Richard Flatman
Anti-bribery policy review			Audit Committee	17 Oct 2017	Richard Flatman
Annual value for money report	Executive	25 Oct 2017	Audit Committee	9 Nov 2017	Richard Flatman
External audit letter of representation	Executive Audit Committee	25 Oct 2017 9 Nov 2017	Board of Governors	23 Nov 2017	Richard Flatman
External audit findings	Executive Audit Committee	25 Oct 2017 9 Nov 2017	Board of Governors	23 Nov 2017	Richard Flatman
Annual report and accounts	Executive Audit Committee Finance, Planning and Resources Committee	25 Oct 2017 9 Nov 2017 14 Nov 2017	Board of Governors	23 Nov 2017	Richard Flatman

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
Quality Assurance return to HEFCE	Quality and Standards Committee Academic Board Audit Committee	4 Oct 2017 1 Nov 2017 9 Nov 2017	Board of Governors	23 Nov 2017	Shân Wareing
Modern Slavery Act statement	Audit Committee	9 Nov 2017	Board of Governors	23 Nov 2017	
8 February 2018					
Corporate risk register	Executive	24 Jan 2018	Audit Committee	8 Feb 2018	Richard Flatman
TRAC return to HEFCE to be ratified			Audit Committee	8 Feb 2018	Richard Flatman
Speak up report			Audit Committee	8 Feb 2018	James Stevenson
Internal audit progress report	Executive	24 Jan 2018	Audit Committee	8 Feb 2018	Richard Flatman
FMI structure and leadership team			Audit Committee	8 Feb 2018	Richard Flatman
Data assurance report	Executive	24 Jan 2018	Audit Committee	8 Feb 2018	Richard Flatman

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
Audit Committee business plan			Audit Committee	8 Feb 2018	Michael Broadway
Anti-fraud, bribery and corruption report	Executive	24 Jan 2018	Audit Committee	8 Feb 2018	Richard Flatman
7 June 2018					
Corporate risk register			Audit Committee	7 Jun 2018	Richard Flatman
TRAC return to HEFCE			Audit Committee	7 Jun 2018	Richard Flatman
Speak up report			Audit Committee	7 Jun 2018	James Stevenson
Internal audit progress report	Executive	23 May 2018	Audit Committee	7 Jun 2018	Richard Flatman
Internal audit plan	Executive	23 May 2018	Audit Committee	7 Jun 2018	Michael Broadway
Indicative pensions assumptions			Audit Committee	7 Jun 2018	Richard Flatman
External audit plan	Executive	23 May 2018	Audit Committee	7 Jun 2018	Richard Flatman

Agenda Item	Consider By	Date	Decision By	Date	Lead Officer
Audit Committee business plan			Audit Committee	7 Jun 2018	Michael Broadway
Anti-fraud, bribery and corruption report	Executive	27 Jun 2018	Audit Committee	7 Jun 2018	Richard Flatman
Anti-fraud policy review			Audit Committee	7 Jun 2018	Michael Broadway
Annual debt write off			Audit Committee	7 Jun 2018	Richard Flatman
Non-regular items					
Apprenticeships update			Audit Committee	3 Oct 2017	Shân Wareing