

Meeting of the Group Audit and Risk Committee

3.00 pm on Monday, 7 September 2020
via MS Teams

Agenda

<i>No.</i>	<i>Item</i>	<i>Pages</i>	<i>Presenter</i>
1.	Welcome and apologies		DB
2.	Declarations of interest		DB
3.	Minutes of the previous meeting	3 - 6	DB
Coronavirus			
4.	Recovery project update September 2020 <ul style="list-style-type: none"> • LSBU alert levels • Face-to-face data collection 	7 - 18	DP
5.	Student advice and behaviours	19 - 22	NL, PB
Internal audit			
6.	Internal audit: cyber security	23 - 72	NL

Date of next meeting
4.00 pm on Tuesday, 6 October 2020

Members: Duncan Brown (Chair), John Cole, Mark Lemmon and Rob Orr

In attendance: Pat Bailey, Alison Chojna, Natalie Ferer, Richard Flatman, Kerry Johnson, Nicole Louis, Marcelle Moncrieffe-Johnson, David Phoenix, Ed Spacey, James Stevenson and Gemma Wright

Internal auditors: Mathew Ring and Gemma Wright (BDO)

This page is intentionally left blank

**Minutes of the meeting of the Group Audit and Risk Committee
held at 2.00 pm on Wednesday, 12 August 2020
via MS Teams**

Present

Duncan Brown (Chair)
John Cole
Mark Lemmon
Rob Orr

In attendance

Pat Bailey
Alison Chojna
Natalie Ferer
Richard Flatman
Asa Hilton Barber
Kerry Johnson
Janet Jones
Nicole Louis
Marcelle Moncrieffe-Johnson (*for minute 5*)
David Phoenix
Ed Spacey
James Stevenson

1. Welcome and apologies

The Chair welcomed members to the meeting.

No apologies had been received.

2. Declarations of interest

No interests were declared on any item on the agenda.

3. Recovery project update August 2020

The committee discussed the overview of measures taken to enable the campus to safely re-open.

The committee discussed the potential security issues arising from the use of personal computers while staff work from home. The Acting Director of Academic Related Resources provided detail of the measures being taken to mitigate risk in this area. The committee noted that a planned internal audit on IT security would be discussed in detail at the meeting of 7 September 2020.

The committee noted the project risk register, guidance on re-opening and remote working guidance, included as appendices.

The committee discussed the accountability for decisions taken at South Bank Colleges and South Bank Academies. It was noted that the Boards of SBC/SBA had considered their respective re-opening plans and associated risks. The Chair requested an overview of the measures taken and it was agreed that the committee would be provided with copies of the relevant minutes.

The Vice Chancellor explained that several student-related aspects of the recovery project were still being finalised, and that this aspect would be covered further at the committee's 7 September 2020 meeting.

Following discussion the committee supported the principles set out within the coronavirus recovery project report, on the basis that a further update would be provided at the next meeting.

4. Academic delivery

The committee considered the processes relating to quality assurance and academic delivery in semester two 2019/20 and semester one 2020/21.

The Provost outlined the actions that had been taken to reassure students and staff that courses could be delivered safely while maintaining academic quality and standards. These actions included the establishment of the Academic Delivery Group (ADG) and the development of alternative assessments. The committee noted that the alternative assessment methods were approved through the Schools' Academic Standards Committees. Required amendments to the academic regulations (such as changes to compensation and condonement rules) were approved by the Academic Board.

Management confirmed that changes to courses for semester one 2020/21 had been documented in compliance with the expectations of the Competition and Markets Authority (CMA).

Following the above discussion the committee agreed that it was happy with the level of assurance provided by the processes for academic delivery.

5. People & Organisational Development update

With Marcelle Moncrieffe-Johnson

The committee discussed the update on the People & Organisational Development (POD) coronavirus recovery project workstreams.

The committee noted that a personal health and circumstances assessment had been sent to all staff, currently with a 55% response rate. Roughly 70% of respondents had confirmed they did not view themselves as vulnerable.

The committee noted that 469 LSBU and SBU EL staff had completed the online return to work training as at 31 July 2020.

The Chief People Officer confirmed that guidance for staff was reviewed and updated on a weekly basis to take account of changing circumstances and government guidance.

The committee noted the continued positive engagement with trade unions.

The committee discussed the need for comprehensive guidance on how academic staff should manage student behaviours and expectations following the implementation of different methods of teaching delivery, and requested an update for its next meeting on 7 September 2020.

Marcelle Moncrieffe-Johnson left the meeting.

6. Recovery project: executive update 5 August 2020

The committee noted the project update, as presented to the Group Executive on 5 August 2020.

**Date of next meeting
3.00 pm, on Monday, 7 September 2020**

Confirmed as a true record

..... (Chair)

This page is intentionally left blank

	CONFIDENTIAL
Paper title:	Covid 19 Update
Board/Committee:	Group Audit and Risk Committee
Date of meeting:	7 September 2020
Author(s):	Ed Spacey, Acting Director of Group Assurance. Daniel Frings, Chair of LSBU Ethics Committee.
Sponsor(s):	David Phoenix, Vice Chancellor and Chief Executive. Patrick Callaghan, Dean and Professor of Mental Health Science in School of Applied Sciences
Purpose:	To provide an update on Covid 19 developments.
Recommendation:	To note the content of the report.

Executive summary

To highlight additional measures being taken to protect staff and student safety, and plans for how the organisation will respond to increases in positive cases of Covid 19.

Note that escalation trigger levels remain under review and ongoing discussion.

To outline a system for returning to face to face research.

This page is intentionally left blank



Covid 19 Recovery Project Update September 2020

1.0 Purpose

- 1.1 To provide the Group Audit and Risk Committee with an update on preparations for campus re-opening.
- 1.2 This builds upon the previous report of 12 August.

2.0 Position on Face Coverings

- 2.1. The previous report highlighted that the Government position on the use of face coverings was continuously changing. After careful consideration and sector analysis, the following decision was reached:
- 2.2. All staff and students are now required to wear face coverings indoors with the following exceptions:
 - a) If you have a medical exemption;
 - b) In eating areas;
 - c) In the Gym as per Government guidance;
 - d) In a single person office with no visitors;
 - e) In your Hall of Residence Flat;
 - f) Limited number of exempt rooms where coverings are not appropriate e.g. studio work. This is risk assessed and clearly communicated by the academic / local manager.
- 2.3. Staff and students will be expected to provide their own face coverings. Limited stocks will be available if people lose their own covering. Front line staff will also be offered the option of visors.

3.0 Second wave / dealing with an increase in cases

- 3.1. In order to be able to respond to changes by national Government, local/regional lockdowns and any increase in numbers of staff /students testing positive, a framework approach has been developed. This is given in **Appendix A**. There is also guidance on moving between LSBU overall preparedness levels vs localised actions. **Appendix B** provides information on face to face research decisions.

4.0 Covid Support Lines

- 4.1 To facilitate any staff on campus to provide comments on covid issues, a helpline will be provided via the Estates Service Desk. This will cover questions ranging from social distancing building markings, to emergency re-provision of hand sanitizer supplies.

LSBU Covid 19 Alert LevelsCurrent Position: **Level 3**Intention to move to **Level 2** - September

	Education	Research	Accommodation	Campus Services	Student Services/SU
Level 5 Full Lockdown	Online only/alternative planning/extend semester inc for Lab based subjects Separate arrangements for NHS placements	All but essential Covid 19 related activities suspended	Remain in campus accommodation if cannot return home - subject to Gov Guidance	Online only, apart from essential EAE staff. Extend semester for Lab based subjects	Online only Emergency online support packages
Trigger from Level 4 to 5 See Guidance	Gov, Regional direction or v.high number of LSBU cases				
Level 4 Restricted operations	Online only/alternative planning/extend semester inc for Lab based subjects Separate arrangements for NHS placements. Staff access requests via EAE, but only by exception	Phased return of any funded or critical research allowed, subject to Exec sign off	Limited use – prioritised to support those who cannot leave	Online only apart from essential EAE staff. Extend semester for Lab based subjects	All online
Trigger from Level 3 to 4 See Guidance	Gov, Regional direction or significant number of LSBU cases				
Level 3 First stage re-opening	Education delivery mainly online delivery, Labs and practicals open following covid secure guidelines	As above	Available to support student need, subject to covid secure guidelines and halls bubbles	Study areas/Library open subject to covid secure guidelines. Clearing operation can take place	Some socially distanced activities, inc induction week

				onsite. Limited PSG staff operate on site	
Trigger from Level 3 to 2 See Guidance	Increasing return to new normal nationally. Covid secure systems working at Level 3				
Level 2 Second stage re-opening	Larger group sessions to resume when safe, following covid secure guidelines. Increasing numbers of academic staff return to campus	Return of research which requires on campus facilities	Full return to accommodation, as social distancing begins to ease.	Delivery of socially distanced services transitioning to full operations. Campus Catering facilities open. Limited Gym facilities open. Increasing numbers of PSG staff on campus	Delivery of socially distanced services transitioning to full operations
Trigger from Level 2 to 1	Covid secure systems working effectively at Level 2. No significant spikes in cases. National guidance being relaxed.				
Level 1 BAU/New normal	All physical classes to resume, alongside any flexible digital delivery	Research activities continue	Full return	Full return	Full return

Guidance on Covid Alert Levels

National Situation /Regional Instruction/Regulator Requirement

Follow all external guidance. In the most extreme cases, this is likely to be a move to Restricted Operations Level 4 or full Lockdown Level 5 depending on severity.

LSBU Internal Situation

The following provides broad guidance for a range of individual situations, and needs to be interpreted depending on the specifics of the situation, and total number of students and staff using the campus at any one time.

Local functions – No change in overall Level.

Response determined by Dean/Director in consultation with Provost/PSG Exec Member.

Multiple student cases in one class or cohort Likely to be 20% + of class/cohort size	Move to online delivery of class material or alternative planning such as module delay Consider School position if numbers increase
Multiple staff cases in same academic discipline. Likely to be 3+, subject to discipline size	Move to online delivery of that discipline or alternative planning such as module delay. Consider School position if numbers increase
2+ staff cases from same School SLT	SLT online service only. Consider wider School position
2+ staff cases from same PSG SLT	SLT online service only. Consider wider PSG position
Multiple staff cases from same PSG or function. Likely to be 20%+ of PSG size.	Move to online service only or alternative planning, depending on size/nature of PSG

Executive. Response determined by remaining Exec members

2+ Executive cases	Move to online service. Consider wider Group position early and review .
--------------------	--

Areas and Buildings

Decisions impacting on major multi use facilities and buildings will need Executive agreement.

Refectory/Café 3+ cases traced to use of same dining area	Close catering facility for sustained period and consider closing other cafes.
15+ cases traced to use of Library	Close Library
15+ cases traced to use of 1 Building	Close specific Building whilst investigate

Cumulative Events

Decisions re cumulative events will need Executive agreement and consideration.

20%+ of total student and staff numbers onsite test positive within 14 days	Move to Level 5 Full Lockdown and review situation
15%+ of total student and staff numbers onsite test positive within 14 days	Move to Level 4 Restricted Operations and review situation
10%+ of total student and staff numbers onsite test positive within 14 days.	Consider Move from Level 2 to Level 3 whilst situation stabilises.

(Total student and staff numbers onsite taken from average data from Track and Trace/Entry system).

Face-to-face data collection during the COVID19 Pandemic

This paper outlines how LSBU can return to undertaking face to face research using a system based on a number of levels of permitted research activity. It allows the institution to move between levels as the external COVID situation wanes and waxes. It includes a description of the levels and permitted research, governance guidance on risk assessment and also details what needs to be included in participant facing documentation. It has received input from colleagues in Health and Safety, Tech services, Govlegal and Data protection.

While the COVID19 situations persists, it is likely that the risk to participants and research staff will vary at different times. One way of adapting to this is have face-to-face data collection operating at one of three levels, with the level of activity dependent on risk. The level can change according to circumstance and go in either direction. The decision to make a level change is to be taken by the Academic Board with a recommendation from URC, based on advice from UEP, REI, H&S, Technical services and RBoS. The current levels of activity should be made prominent on Haplo, and changes announced by the Provost.

Level 4: Face-to-face data collection moratorium

1. No face-to-face data collection permitted.

Level 3: Social distancing research only

1. Only face-to-face research in which social distancing can be maintained can be conducted. Research requiring close contact (i.e. in which social distancing is not possible) remains under the moratorium
2. The following should not take part in face-to-face research as participants or data collecting researchers:
 - Clinically extremely vulnerable or clinically vulnerable people
 - People who have travelled abroad in the last 14 days
 - People who are displaying COVID19 symptoms
 - People living in a household where someone else has displayed symptoms in the last 14 days.

Consideration as to exclusion should be given to BAME status of participants over 55 or with co-morbidities.

3. A risk assessment should be conducted by the research team intending to carry out the work and confirmed with a competent member of staff someone outside the research team (usually, lab technicians) following the guidelines below.
4. No physical contact between individuals (including, for instance, handshakes etc).
5. Unless current advice contradicts this policy, PPE may be excessive outside of clinical and care environments. If face coverings (*note, these differ from respirator masks which are not recommended outside of healthcare settings*) are going to be implemented as a control measure, wearers should be instructed on safe wear, securing, removal, cleaning and hand washing procedures.

6. The research team should add the following statement to the risks of taking part section of the study Participant Information Sheet; *'You will be visiting a lab which is an indoor public space. While we are actively minimising the risk of COVID19 transmission in these spaces, there is an increased risk of contracting the virus if you take part in the study. The research team can provide details of the study control measures in place to address safety on request.*
7. Participant information sheets should include the following exclusion criteria
'This study is not open to:
 - *Clinically extremely vulnerable or clinically vulnerable people or individuals who live with such people*
 - *People who have travelled abroad in the last 14 days*
 - *People who are displaying COVID19 symptoms or have in the last 7 days*
 - *People living in a household where someone else has displayed symptoms in the last 14 days*
8. Consent forms should include the following opt-ins *'I confirm I am not a member of any of the groups listed as excluded in the information sheet.'* and *'I consent for LSBU to hold data about my study participation and share this with outside agencies for the purpose of COVID19 infection tracking (i.e. with 'track and trace' teams). I understand that withdrawal from the study will not lead to data relevant to track and trace being destroyed.*
9. Amended documentation should be lodged on Haplo as an amendment, highlighting the sections which have been altered. An approval from the relevant UEP should be given before research commences.

Level 2: Close contact research resumes

1. Research involving personal physical contact can be conducted.
2. Research which involves physical contact should not include clinically extremely vulnerable or clinically vulnerable people as participants. For research in which social distancing is possible, these populations are eligible for research participation. The remaining exclusion criteria from Level 3 and the need to consider BAME status for those over 55 or with co-morbidities still apply in both cases.
3. A risk assessment should be conducted by the research team intending to carry out the work and confirmed with a competent member of staff someone outside the research team (usually, lab technicians) following the guidelines below.
4. For studies where researchers and participants are in close proximity, the use of PPE should be considered. These should be used to manage residual risk after other controls have been implemented.
5. Participant information sheets should add the following statement to the risks of taking part section *'You will be visiting a lab which is an indoor public space. While we are actively minimising the risk of COVID19 transmission in these spaces, there is a risk of*

contracting the virus if you take part in the study (as with any contact between people). The research team can provide details of the study control measures in place to address safety on request.'

6. Participant information sheets should include the following exclusion criteria
'This study is not open to:
 - *Clinically extremely vulnerable or clinically vulnerable people or individuals who live with such people* [note, for social distance studies this clause can be dropped]
 - *People who have travelled abroad in the last 14 days*
 - *People who are displaying COVID19 symptoms or have in the last 7 days*
 - *People living in a household where someone else has displayed symptoms in the last 14 days.*
7. Consent forms should include the following opt-in *'I confirm I am not a member of any of the groups listed as excluded in the information sheet.'* and *'I consent for LSBU to hold data about my study participation and share this with outside agencies for the purpose of COVID19 infection tracking (i.e. with 'track and trace' teams). I understand that withdrawal from the study will not lead to data relevant to track and trace being destroyed'.*
8. A clear statement of the level of close contact should be included in the Participant Information Sheet.
9. Participants' status as clinically vulnerable or extremely clinically vulnerable should be recorded.
10. Amended documentation should be lodged on Haplo as an amendment, highlighting the sections which have been altered. An approval from the relevant UEP should be given before research commences.

Level 1: Routine

1. Social distancing consideration and PPE considerations part of the review process. Clinically vulnerable people can be considered for inclusion on the basis of beneficence. Clinically extremely vulnerable remain excluded from face-to-face research.
2. Amended documentation should be lodged on Haplo as an amendment, highlighting the sections which have been altered.

Control measures during Levels 1, 2 and 3 should include as a minimum:

- Active consideration of the suitability of the room in terms of size and ventilation
- Have tissues, suitable hand sanitiser (70%+ alcohol content) available and serviced (i.e. regularly emptied) bins close-by
- Sign-post hand-washing sites (some labs have hand-washing facilities)
- Careful positioning of participants and researchers so they exhale away from each other (including seating multiple people side by side)
- Researcher temperature checks at start of each days testing sessions
- Scheduling of participants to ensure minimal inter-participant contact

- Sanitising of room between participants where possible
- Securely held (double lock) logs of who contacts are made with and when (i.e. which participants and which researchers) held for three months.
- Wiping down of pens, clipboards or other materials touched by participants or other researchers between participants
- Any additional health and safety or technical service advice.

Lab managers, researchers and risk assessors should also consider:

- Use of larger lab to allow physical distancing
- Use of screens, barriers etc
- Added ventilation in the lab
- Limiting non-social distance time to 15 minutes
- Any additional health and safety or technical service advice

(in particular; <https://www.gov.uk/guidance/working-safely-during-coronavirus-covid-19/labs-and-research-facilities>)

This page is intentionally left blank

Agenda Item 5

	CONFIDENTIAL
Paper title:	Student Advice and Behaviors in Relation to Covid 19
Board/Committee	Group Audit and Risk Committee
Date of meeting:	7 September 2020
Author:	Rosie Holden – Director of Student Services (Employability, Sport, Wellbeing)
Sponsor:	Nicole Louis – Chief Customer Officer Pat Bailey - Provost
Purpose:	To Note
Recommendation:	The committee is asked to note the safety precautions and expected behaviors that have been communicated to students in relation to Semester 1 return to campus

Executive Summary

The attached document contains information that has been provided to students in relation to safety precautions undertaken by LSBU to ensure that the campus is Covid Safe, and the responsibilities and behaviors expected of them to contribute to campus safety.

Please note that student conduct in relation to Covid 19 precautions is governed by the University's existing Student Disciplinary Procedure (updated June 2020). The first principle contained within the procedure document states that:-

‘All University staff, students, contractors and visitors have a right to work, study and learn in a safe environment and any conduct which unreasonably interferes with the safe and orderly operation of the University community will be investigated and addressed in accordance with this procedure’.

In addition, Appendix A of the procedure document sets out specific examples of misconduct which, if proven, may amount to a disciplinary offence leading to formal disciplinary action under this procedure. In relation to health and safety, the Appendix lists the following example of misconduct:-

‘putting the health and safety of yourself or others at significant risk’

Staying safe on campus

We look forward to welcoming you to campus - we know we'll all need to support each other as we get used to new ways of studying and working.

How we're protecting you

- full risk assessment of buildings and on-campus activities
- asking staff, students, and visitors to wear a face covering and observe 2m social spacing
- fewer people on-site, extended teaching hours, and 2m social spacing in teaching rooms
- new entrances, exits, and one-way systems
- protective screens
- cleaning stations and hand gel dispensers for all entrances, teaching rooms, and facilities
- increased cleaning on campus
- monitoring possible cases of Covid-19 to keep the community safe using the [SafeZone app](#)

Keeping yourself and others safe – your responsibilities

Don't come to campus if you or anyone in your household has Covid-19 symptoms – self-isolate and arrange a [free NHS test](#) as soon as possible. Use the [NHS 111 online coronavirus service](#) if your symptoms get worse.

Download the [SafeZone app](#) to receive up to date safety information from LSBU and to report if you have symptoms.

On campus

- Try to come to campus only on days when you have timetabled on-site teaching or need to use campus facilities such as the library or study support areas, Academy of Sport or access face-to-face support services
- Use a face covering when inside any LSBU building (unless you are eating or drinking, exercising in the gym, on your own in a single office or in your own room in halls of residence, or [you are exempt](#))
- Follow Government [social spacing guidance](#) by keeping to 2m distance wherever possible
- Be patient when waiting to enter/exit a teaching room and keep a safe distance apart
- Before you use a desk, table, or computer on campus, clean the surface with the products provided
- Follow signs on campus for entrances, exits, one-way routes and [handwashing guidance](#) and follow specific guidance for spaces such as laboratories and workshops
- If you are able to use the stairs, please do so and keep lifts available for those who are unable to use the stairs
- Regularly wash your hands with soap and water, and use hand sanitizer (provided across campus)
- Don't touch your face, and use a tissue if you cough or sneeze – then throw it in a bin

If you develop symptoms

It's important to tell us if you [develop symptoms](#) so that we can keep you and everyone safe

If you're on-campus, go straight home to self-isolate and arrange an NHS test

If you're off-campus, self-isolate at home and arrange an NHS test

For everyone, make a report to LSBU using the [SafeZone app](#). If you don't have a smartphone and can't use the app, email covidreport@lsbu.ac.uk to let us know. We will be in touch to make sure you're ok, and advise you if you need to do anything else

Support for you and being supportive to others

In these unsettling times, it's ok to feel anxious or upset.

If you have a question about anything that's worrying you, or you just want someone to talk to, contact us at the Student Life Centre studentlife@lsbu.ac.uk

You may have a health condition or personal circumstances that mean you are considered clinically vulnerable or extremely clinically vulnerable. To make sure you're well supported in your studies and that we identify any actions we can take to support you, please contact studentwellbeing@lsbu.ac.uk

Remember, there are lots of reasons why someone may be unable to use a face covering which may not be obvious to you – there is no requirement for someone to provide evidence of exemption. Don't challenge someone who isn't wearing a face covering – it should be assumed there is a legitimate reason why they cannot.

Channels of communication

- Published guide for students using the above information as the basis
 - Long version (similar to staff RTW guide)
 - Short version (digital and printed versions)
 - Video
 - Social media posts
 - Additional posters/banners as required around the campus
 - Standard PowerPoint slide (top tips and SafeZone) to be shared with course teams to use at start of every lecture
- Campus spaces
 - Posters around the campus
 - Content on digital screens
- SafeZone (safety app) specific comms
 - What it is, what it does, why to download, how to download
 - Posters and banners esp. for Halls
 - Social media snapshots
- Welcome Week
 - To include a short student guide and video to the Welcome Week site and to the Welcome Week checklist (what you need to know, download SafeZone)
 - Include content in 'Safety and Security Session'
 - Guidance and SafeZone app info at every Welcome Week Gazebo and given out at face-to-face and through online enrolment
- Halls
 - Halls meetings to include SafeZone and reminder of safety advice
 - Posters for every flat in halls of residence
- Communication schedule
 - New students Aug – Sept (what you need to know, download SafeZone)
 - Continuing students Aug – Sept (what you need to know, download SafeZone)
 - All students from September onwards...

End

Agenda Item 6

CONFIDENTIAL - RESTRICTED TO MEETING PARTICIPANTS	
Paper title:	BDO Cyber Security Audit Report
Board/Committee:	Group Audit and Risk Committee
Date of meeting:	07 September 2020
Author(s):	Alison Chojna, Acting Executive Director of Academic Related Resources
Sponsor(s):	Nicole Louis, Chief Customer Officer
Purpose:	For Review
Recommendation:	The committee is requested to review the information provided and management responses.

Executive summary

In May 2020, a cyber security assessment of the LSBU Group was undertaken by external auditors, BDO. The following report details the findings and recommendations, along with the management responses. The majority of findings were well understood at the time of the audit and were either in the process of being remediated or plans were in place to do so.

31 findings were identified in total; seven of high significance, 22 of medium significance and two with low significance have been raised across all three entities. Several are common across the Group and can be remediated at the Group level. They are distributed as follows:

	High	Medium	Low
LSBU	4	8	0
SBC	2	7	1
SBA	1	7	1

The level of assurance for operational effectiveness is rated as “limited assurance as a result”.

BDO are supportive of the 5yr Group IT Strategy which moves to an integrated IT infrastructure and centralised IT functions as part of the target operating model. Roles associated with cyber security will transition to a centralised Group structure, supporting a unified approach to various cyber security concerns, such as threat detection, incident management, training & awareness, security design and governance of policies and processes. The Head of IT Security role can be transitioned quickly but supporting roles will require change proposals at both LSBU and SBC to make space in the staffing structures.

The most significant existing risk relates to the configuration of the current network at LSBU, which is flat. Best practice would introduce demilitarised zones (DMZs) to separate systems with specific security requirements from internal networks and untrusted networks. A redesign of the network is planned as part of the upcoming network replacement and should be in place by early 2021.

This page is intentionally left blank

LONDON SOUTH BANK UNIVERSITY GROUP

INTERNAL AUDIT REPORT - FINAL

INFORMATION SECURITY
AUGUST 2020

	LEVEL OF ASSURANCE	
	Design	Operational Effectiveness
LSBU	Limited	Limited
SBC	Moderate	Limited
SBA	Limited	Limited



LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

EXECUTIVE SUMMARY	2
DETAILED FINDINGS	8
OBSERVATIONS	41
STAFF INTERVIEWED	42
APPENDIX I - DEFINITIONS.....	43
APPENDIX II - TERMS OF REFERENCE	44

DISTRIBUTION

Nicole Louis	Chief Customer Officer
Alison Chojna	Acting Executive Director of Academic Related Resources







REPORT STATUS LIST

Auditor:	Goran Bonevski
Dates work performed:	11 - 30 May 2020 - closing meeting 4 June 2020
Draft report issued:	14 June 2020
2 nd Draft issued	24 August 2020
Final report issued:	27 August 2020

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

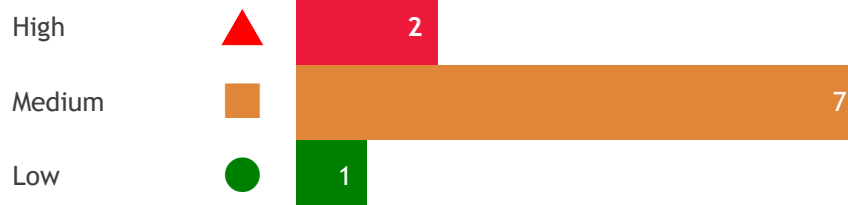
LSBU	Design	 System of internal controls is weakened with system objectives at risk of not being achieved.
	Effectiveness	 Non-compliance with key procedures and controls places the system objectives at risk.
SBC	Design	 Generally a sound system of internal control designed to achieve system objectives with some exceptions.
	Effectiveness	 Non-compliance with key procedures and controls places the system objectives at risk.
SBA	Design	 System of internal controls is weakened with system objectives at risk of not being achieved.
	Effectiveness	 Non-compliance with key procedures and controls places the system objectives at risk.

LSBU UNIVERSITY SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)



TOTAL NUMBER OF RECOMMENDATIONS: 12

LAMBETH COLLEGE SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)






TOTAL NUMBER OF RECOMMENDATIONS: 10

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

ACADEMIES

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High		1
Medium		7
Low		1

TOTAL NUMBER OF RECOMMENDATIONS: 9

BACKGROUND:

London South Bank University Group (the Group) is a specialist education provider that includes London South Bank University (LSBU University), Lambeth College (SBC), South Bank University Academy of Engineering (UAE) and South Bank University Engineering UTC (SBA).

In accordance with Group's 2019/20 Internal Audit Plan, BDO has undertaken an audit of Information Security across the Group.

The objective of this audit was to provide independent and objective assurance on the adequacy and effectiveness of information security activities. These activities are aimed at protecting data, information and related ICT infrastructure, for the systems, processes and services managed at the audited entities.

Separate Active Directory (AD) instances and networks are implemented in all audit entities. There is a decentralised approach to the delivery of information security and IT services.

Despite the fact that there is little inter-connectivity on the IT level between the entities, they have similar risks profiles.

Complex IT estates can be difficult to support and problematic to transform due to the interdependencies between systems. The IT department focuses on the maintenance of the system instead on innovation, as stated in the LSBU Group IT Strategy 2020-2025. As a consequence of the similar risk profiles, similar findings have been identified at the all entities during this review. The Group is aware of this issue, and has started IT service integration and modernisation initiatives with the aim to develop a more agile hybrid cloud based future operating environment.

The recommendations in this report are aligned to the LSBU Group initiatives of integration and modernisation. The LSBU's intention to develop a more agile operating environment will face additional challenges without a applying a consistent standard of security best practice across the Group.

LSBU

LSBU's ICT arrangements are managed centrally. The Head of Information Security is positioned separately with direct responsibility to the Executive Director of Academic Related Resources.

A third party has recently undertaken penetration testing at LSBU and Lambeth College.

SBC

Lambeth College's Leadership Group is responsible for approving the IT Security policy and for ensuring that it is implemented College wide. The College's Director of IT and Resources is responsible for day to day information security operations as well for coordinating investigations into any reported IT security incidents.

SBA

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

IT services and security for the Academies is outsourced to Pallant Management Services Ltd.

SCOPE AND APPROACH:

Across the Group the review considered:

- **Identify** - Information security policies, standards procedures and strategies, as well as risk assessment processes, cyber threat intelligence gathering, security governance and training / awareness
- **Protect** - Design of the network (isolation and segmentation), as well as the management of key controls such as perimeter (firewall) configuration, access restrictions, asset management (including mobile assets) and cryptograph
- **Detect** - Threat detection controls, such as for intrusion detection systems (IDS) and antivirus/malware tools
- **Respond** - Security event and incidents management processes
- **Recover** - Data backup/restore, fail-over and recovery processes.

As part of the Protect section, we identified the information security perimeter and the information entry and exit points (IT and non-IT based). We considered the corresponding controls in place to manage threats, and the risks of data leakage at each point. This supported us in identifying control gaps and infrastructure components that are vulnerable to attack.

As part of the Recover section, we considered business continuity and disaster recovery plans, facilities and systems, and the protection afforded to the data held within them as well as the effectiveness of the recovery measures in supporting continuity after a cyber-attack.

We considered the information/cyber security controls in alignment with the (US) National Institute of Standards and Technology (NIST) cyber security framework.

Our approach was to conduct interviews to establish the controls in operation for each of our areas of audit work.

In order to remain compliant with COVID-19 guidelines, we performed this review remotely using a combination of video conferencing and email.

GOOD PRACTICE:

As a result of our review we have identified the following areas of good practice:

LSBU

- There is a dedicated information security role
- The Information Security policy and other relevant policies follow the ISO 27001 recommended structure and the University is planning on gaining the Cyber Essentials certification.
- Information security pages are present on the University's intranet portal
- There is a Software as a Service (SaaS) Security Checklist
- Identity lifecycle management is in use
- There is regular reporting on managed network services
- The University has a wide-ranging IT service catalogue.

SBC

- There is a detailed Information Security policy in place
- There is good network segregation and segmentation
- The College's networks are well documented
- There are full infrastructure and application inventories

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

- Password complexity and longer passwords are enforced for all staff.

SBA

- There is good network segregation and segmentation
- IT/data security risks are present in the risk register
- South Bank University Academy of Engineering has a set of IT and information security policies
- Anti-virus is installed on workstations and servers
- The network is monitored using network monitoring software.

KEY FINDINGS:

31 findings; seven of high significance, 22 of medium significance and two with low significance have been raised across all three entities.

This was the first Cyber Security Review at the entities, so the relative high number of findings is typical to organisations with a similar size and risk exposure. It should also be noted that this is a report covering three different entities with different IT infrastructure.

End-of-life infrastructure and operating systems as well as the lack of an information security management framework also contribute towards the volume of findings.

The distributions of findings by entity is as follows.

Group

Although the review was limited to the three entities, improvements noted in the report relating to the information security governance finding need to be elevated to the highest Group levels. The Group plans for further integration of the IT function and systems are another strong argument for hosting a Group information security governance framework that will drive the processes of Information Security.

Recommendations linked to this finding mean that the board and various levels of management should be regularly informed about information security risks and also informed about the implementation and design of security measures. This will ensure improved alignment of information security to the business needs and optimisation of information security investments.

We have noted security risks which are shared between the entities. As part of the plans for further integration, remedial action for these issues could be managed at a Group level. These areas are:

- Asset Management (Recs 9, 15, 25)
- Access Control, (Recs 8, 20, 29)
- Security Awareness (Ref 22, 31)
- Penetration testing and vulnerability scans (Ref 18, 27)
- Incident Management (Ref 10, 19)

LSBU

At the University we have raised 12 findings; four of high significance and eight of medium significance.

Besides the high ranked information security governance finding noted above, we identified critical areas of improvement in the security controls associated with anti-virus and password control implementation. These two controls are considered basic security hygiene and need to be addressed with a high priority. The last high ranked finding is related to the flat design of the network (which means the network is not segregated to provide increased control), that opens the internal network to untrusted networks and intranet.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

The medium ranked findings relate to the weaknesses in the technical controls as there is unrestricted use of USB devices, presence of obsolete operating systems and poor administration of local administrator accounts.

Moderate weaknesses are also identified in LSBU framework's related to security incident response, lack of a formal patch management policy, information security asset management and formal and consistent review of access rights.

Other medium findings relate to recovery abilities. Improvement is needed in the backup design and implementation and also business continuity and disaster recovery plans.

SBC

At Lambeth College we raised ten findings; two of high significance, seven of medium significance and one of low significance.

The two high ranked findings are related to the presence of end-of-life operating systems and network equipment. The main IT services and core network devices are obsolete and significantly increase the likelihood of cyber security incident occurring.

The medium findings relate to patch management, lack of regular penetration testing and review of users accounts and missing anti-virus installation on the servers.

Additional improvements are also required in the documentation of information security asset management, incident management and backup/resilience plans.

SBA

For the academies we raised nine findings; one of high significance and seven of medium significance and one of low significance.

The high finding relates to poor implementation of password controls, in an environment with a large number of users with weak passwords, this significantly increases the likelihood of user account compromise.

The medium findings relate to the limited capacity of the network backbone, absence of regular penetration testing, deficiency in formal access control policy, lack of a formal asset management framework, no off-site storage of the backups and weak physical access control at South Bank University Engineering (UTC) server room.

At UTC we noted that there is no information security policy or other documents relating to information security management.

CONCLUSION:

Group

While areas of good practice exist, they are not consistent across the group. Group objectives and minimum requirements have not been defined and communicated, therefore there is no single 'truth' for security operations to implement.

Achieving an effective and consistent standard approach to information security throughout the organisation requires clear direction from the top.

LSBU

LSBU has implemented a number of good practices to mitigate information security risks. However, we have noted a number of areas of improvement and as a result the design and operational effectiveness of the controls are rated as 'limited'.

SBC

Critical weaknesses have been identified relating to the network devices and operating systems in use. More positively there is a comprehensive information security policy in

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

place. Therefore, we are able to provide moderate assurance over the design of the controls in place and limited assurance over the operational effectiveness of the information security controls in place.


SBA

Whilst basic network security controls are in place, overall we have identified a number of improvement opportunities mainly related to the resilience capability at the academies and the information security management framework. As a result we are able to provide limited assurance over the design and operational effectiveness of the information security controls in place.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

DETAILED FINDINGS - LSBU

RISK: SYSTEMS AND INFORMATION ARE INSUFFICIENTLY PROTECTED AS A RESULT OF A LACK OF GOVERNANCE AND ACCOUNTABILITY OVER INFORMATION/ CYBER SECURITY OPERATIONS.

Ref	Sig.	Finding
1		<p>Modern governance practices no longer consider information security as a technical discipline delegated to specialised services, but as a function that facilitates information security efforts at the highest level.</p> <p>We reviewed the information governance practices in LSBU and we noted the following:</p> <ul style="list-style-type: none"> • There are no information security governance structures that would be typically associated with a fully functioning Information Security Management System. • There are no periodic assessments of information security risks. <p>We reviewed the Head of Information Security job specifications and noted that his responsibility is limited only to information security operation at the University. Furthermore, roles and responsibilities related to the LSBU Group Information Security are not defined.</p> <p>As part of our review, the Head of Information Security presented a Cyber Security Roadmap. However, a formal Information Security Strategy, as a declaration of information security objectives does not exist.</p> <p>We noted that information security policies introduced in the last year are approved by the IT Senior Management Team, which includes the Group Director of IT and the Director of Academic Related Resources, but older information security related policies have been approved by the Operational Board or Deputy Director of ICT services. There is no formal and consistent path of approval, development and maintenance of information security related policies.</p> <p>We were informed that there is ad-hoc monitoring of security performance for the LSBU Group.</p> <p>The tone at the top must be conducive to effective security governance. Visible and periodic board member endorsement of security practices provides the basis for ensuring that information security expectations are met at all levels and entities of the organisation.</p>

RECOMMENDATION:

An information security governance framework should be introduced at Group level that should consist of:

- An information security risk management methodology
- An effective security organisational structure
- A comprehensive security strategy explicitly linked with business and IT objectives
- A process to ensure continued evaluation and update of security policies, standards, procedures and risks
- Security policies that address each aspect of strategy, control and regulation
- Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

MANAGEMENT RESPONSE:

LSBU Group is in the early stages of transition from multiple local IT teams working independently to a target operating model of a unified IT department organised around functional teams rather than mixed-discipline local teams. So far the IT team at SBC has changed management reporting lines to LSBU and the next stage of the transition will be to integrate the teams. It is expected that IT at SBA will continue to be outsourced for some time to come.

The University is the only Group entity with a dedicated resource with responsibility for IT security. In SBC and SBA, responsibility for IT security rests with the IT teams. As a result, at SBC/SBA the technical elements of security are managed but the related people and process elements are not given due attention. Until now, the IT security arrangements have been self-assessed within those teams. At LSBU, the Head of IT Security does report outside of the IT Department to the Acting Executive Director of Academic Related Resources, which provides the opportunity for independent challenge to IT.

LSBU Group will now make the transition to a centralised Group information security governance framework. The Head of IT Security role will be refocussed to a Group security lead with a small team to support the activity. Whilst the change to the Head of IT Security role can be brought about relatively quickly, a change proposal will be required to put the additional supporting roles in place.


A Compliance Board [name TBC] will be established, with representation from across the Group and importantly, including membership from outside of the IT Team as well as IT Leadership. Once established, the Board will oversee and monitor the implementation of the 5 other recommendations outlined in this finding. The Chair of the Board will report quarterly to the Group Executive Committee and the Group Audit and Risk Committee.

Responsible Officer: Alison Chojna, Acting Executive Director of Academic Related Resources

Implementation Date: 31/10/2020 - Head of IT Security role revised to include Group responsibility.
31/10/2020 - Compliance Board established.
01/01/2021 - New governance structure in place, including supporting roles.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES

Ref	Sig.	Finding
2		<p>We reviewed the current design of the University IT network and noted that the trusted zone of the network is flat.</p> <p>The risk is that the systems most vulnerable to attack, such as e-mail, web servers and Domain Name System (DNS) servers are facing an increased level of threat because they are directly exposed to untrusted networks.</p>

RECOMMENDATION:

Demilitarised Zones (DMZs) should be incorporated in the current network design to separate systems with specific security requirements from internal networks and untrusted networks. In addition, firewalls should be employed in a manner that prevents them from being bypassed.

A DMZ is a network (physical or logical) used to connect hosts that provide an interface to an untrusted external network - usually the internet - while keeping the internal, private network - usually the corporate network - separated and isolated from the external network.

MANAGEMENT RESPONSE:

The planning work to redesign and replace the existing network at LSBU and SBC has been progressing over the course of 2019/20. A vendor has been chosen and a tender for the redesign and managed service is about to be issued, with a new supplier expected to be place by December 2020.


The new network will be designed to the latest security standards, including demilitarised zones as recommended above.

Responsible Officer: Alex Denley, Director of Innovation & transformation and James Rockliffe, Director of Procurement Services (responsible for the successful procurement of the new network technology and service).
Graeme Wolfe - Head of IT Security (responsible for ensuring the network design is secure).

Implementation Date: 01/12/2020 - Tender awarded and new managed service contract begins.
31/03/2021 - Core network redesigned and installation complete

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON "NEED TO KNOW" AND "LEAST PRIVILEGE" PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE.

Ref	Sig.	Finding
3		<p>We reviewed the Default Domain policy applied on the University domain lsbu.ac.uk and noted that the policy does not require complex passwords and the password maximum age is set to 365 days. These settings do not follow the recommended security best practice for password control implementation.</p> <p>In addition, we were informed that there is no formal password policy that defines the requirements for password usage.</p> <p>An authentication mechanism is only as strong as its credentials, so weak password requirements make it easier for attackers to compromise user accounts.</p>

RECOMMENDATION:

A formal password policy should be enforced on all systems and users in scope, following the current best practice:

- Set complexity requirements including the use of certain character types (mixed case, numerals and special characters)
- Require passwords to be changed frequently.

MANAGEMENT RESPONSE:

A draft password policy has been developed and is awaiting formal approval. The policy includes the requirement for complex passwords and this will be introduced before semester one commences.

As explained in the audit, the normal password expiry age is 180 days but this was temporarily adjusted during the Covid19 lockdown due to the challenges of remote password reset after expiry. This will be changed back as staff begin to return to campus.


The change to password complexity will be phased in on expiry of individual passwords. The Group Director of IT Services will confirm whether it is possible to accelerate the change by forcing password changes in batches, without putting unacceptable pressure on the network.

Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 11/09/2020 - Password policy approved.
18/09/2020 - Password complexity introduced

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SECURITY IS COMPROMISED DUE TO INADEQUATE REPORTING, LOGGING AND RESOLVING OF IT SECURITY INCIDENTS/EVENTS

Ref	Sig.	Finding
4		<p>The primary purpose of anti-virus solutions or software is to guard against malicious software and alert administrators when malicious software is identified.</p> <p>We were informed that the current Sophos anti-virus solution installed at the University has problems with the reporting of detected issues. An external Sophos review was undertaken in 2019 to identify the root cause of the issues. The review identified issues with the configuration of the software. Sophos recommended a complete re-structure of the anti-virus solution, but this was never actioned.</p> <p>Misconfiguration of the anti-virus solution increases the risk that information security will be compromised as a result of inadequate protection against malware.</p>

RECOMMENDATION:

Installed antivirus protection should be restructured to enable real time detection and prevention against malware.

MANAGEMENT RESPONSE:

The Head of IT Security will confirm whether internal IT Services staff have the required knowledge to undertake the remedial works. If not, an external consultant will be commissioned to undertake the work.


There is a lack of institutional knowledge regarding the existing configuration.

Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 30/11/2020 - To complete the review and identify resource. Work to commence from this date.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LSBU UNIVERSITY IS NOT ABLE TO RECOVER FOLLOWING A SECURITY INCIDENT - THERE ARE NO MEASURES IN PLACE THAT SUPPORTS RESILIENCY OBJECTIVES

Ref	Sig.	Finding
5		<p>The main bulk of the backups are based on business logic. Data domain devices have been used for backup storage.</p> <p>We noted that the backup is running at around 75-90% of capacity and there is no off-site backup copy.</p> <p>Some recovery scenarios have been tested, but regular backup testing is not performed.</p> <p>There is a risk that backup and recovery practices for the information systems are not adequate to support the provision of key business services.</p>

RECOMMENDATION:

The University should formally introduce a backup policy that outlines the backup requirements and specifications for the different systems. Aspects of systems' criticality and data prioritisation should be considered.

Backup and restore plans should be developed according to the result of the business impact analysis. These plans should be formally approved by business management.

The backup retention periods should be formalised in correlation with retention periods defined by legal or business requirements.

Representative samples from the backups (e.g. system images, database, files) should be tested on a regular basis (e.g. at least annually). The results from the restores should be documented and any deviations analysed.

MANAGEMENT RESPONSE:

A backup policy needs to be developed and implemented at a Group level, as each part of the Group is in a similar position. The last backup policy on record was revised in 2006. At LSBU, regular backups are performed but there currently is not an offsite backup or regular testing. This needs to be addressed.


A project will be instigated to plan the backup strategy for the Group, including what should be backed up, where it will be backed up, how often, responsibility and monitoring. The strategy will be approved by the Group Executive.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 30/11/2020 - Backup Strategy has been developed for the Group, with costs identified and approved by the Group Executive.
01/12/2020 - Implementation begins. Duration will be defined by the strategy.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION COMMUNICATED INTERNALLY/EXTERNALLY IS NOT SUFFICIENTLY PROTECTED RESULTING IN EXPOSURE OF SENSITIVE DATA

Ref	Sig.	Finding
6		<p>Windows Server Update Services (WSUS) is used to manage the distribution of updates and hotfixes released for Microsoft products in the University environment. Legacy server and desktop operating systems are patched to the last available update.</p> <p>While a business tier logic is used to prioritise the application of the servers patched, there is no formal patch management policy.</p> <p>The lack of a formal patch management policy increases the risk of attackers exploiting vulnerabilities in systems.</p>

RECOMMENDATION:

A formal patch management policy should be developed to describe the requirements for maintaining up-to-date operating system security patches and software version levels on all the University owned estate and services supplied by third parties.

MANAGEMENT RESPONSE:

A patch management policy has been awaiting approval and will be signed off shortly.


A project to bring the patching up to date is near completion. In recent years it has been carried out on an ad-hoc basis and is at risk of being deprioritised when workloads increase. The patching policy introduces a monthly patching cycle. This will be reported as a KPI at the Compliance Board when in place.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 31/08/2020 - Patch management policy approved.
30/09/2020 - New patch management activity commences, and reporting begins

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION COMMUNICATED INTERNALLY/EXTERNALLY IS NOT SUFFICIENTLY PROTECTED RESULTING IN EXPOSURE OF SENSITIVE DATA

Ref	Sig.	Finding
7		<p>There is no restriction on the use of personal media such as USB drives at the University. In addition we were also informed that there is no mandatory encryption of such drives.</p> <p>USB flash drives pose two major challenges to information system security; data leakage owing to their small physical size and as a method of introducing malicious software into University systems.</p>

RECOMMENDATION:

USB usage should be restricted based on the business needs and risk assessment. In addition USB encryption based on risk should be introduced.

MANAGEMENT RESPONSE:

This recommendation is currently under review to identify the most appropriate and proportionate response in a complex, HE environment. The biggest concern with USB usage is the risk of introducing malware onto University systems. There are a number of methods to reduce this risk under consideration, ranging from complete lockdown of USB ports to automatic antivirus scanning for any device connected via USB.


Both staff and student behaviour need to be considered and by enforcing one solution, we need to ensure that we do not inadvertently introduce an alternative behaviour that carries a greater risk.

Responsible Officer: Alison Chojna, Acting Executive Director of Academic Related Resources.

Implementation Date: 30/11/2020 - Review of options for control of USB devices presented to the Group Executive with recommendations and associated costs.
01/12/2020 - Implementation of chosen solution, duration dependent on the approach selected.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON “NEED TO KNOW” AND “LEAST PRIVILEGE” PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE.

Ref	Sig.	Finding
8		<p>Local administrator accounts on workstations and servers are often needed for management purposes.</p> <p>We noted that the local administrator account is not disabled on all computers in the University IT estate and local administrator passwords are not managed.</p> <p>Compromised local administrator accounts on computers in the secure perimeter increases the risk of further escalation of security compromises to other more sensitive computers and services.</p>

RECOMMENDATION:

IT should disable the local administrator accounts on all computers on University computers.
IT should deploy a Microsoft Local Administrator Password Solution (LAPS) to handle the Local Administrator passwords.

MANAGEMENT RESPONSE:


Local administration accounts are controlled and regularly updated on the desktop devices and servers. All laptop users do have local admin permissions. This needs to be reviewed as a change will increase the support overhead on IT Services staff. A clearly defined policy will be put in place.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 30/11/2020 - Analysis complete to understand the additional support burden on IT Services if this change is made.
01/12/2020 - Report options to Group Executive and agree the future policy.
01/01/2021 - Begin implementation of new policy.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION ASSETS ARE INADEQUATELY SECURED AS A RESULT OF WEAK IT ASSET MANAGEMENT PROCESSES WHICH DO NOT ENSURE THAT IT ASSETS ARE IDENTIFIED, RECORDED, TRACKED AND CLASSIFIED

Ref	Sig.	Finding
9		<p>The ICT Asset Management policy has been in draft since 2017. Snow (an asset management tool) is used to track hardware and software. The IT department is currently updating and reviewing the accuracy of the information Snow captures.</p> <p>We understand that ownership of information security assets is not formally assigned and the concept of asset custodian is not used.</p> <p>We also noted that a system of recording the information security value of the assets and their criticality is not implemented or formalised.</p>

RECOMMENDATION:

The ICT Asset Management policy should be re-reviewed, and additional supporting procedures and processes for asset identification, asset prioritisation and asset classification, ownership and lifecycle should be developed.

An information security asset inventory for all University owned assets should be established. For each identified asset, ownership of the asset should be assigned with a corresponding classification level.

This process could be applied to all Group assets as plans for integration evolve.

MANAGEMENT RESPONSE:

An ICT Asset Management policy will be adopted at a Group level, moving towards a single pane of glass to manage all Group ICT assets.


Work is currently underway to clean the existing asset data from the software tool, SNOW. A programme of works will be planned and approved by Nicole Louis to remediate poor quality data for existing assets, develop the Group ICT Asset Management Policy, identify the appropriate tools to manage this across the Group and identify the staff resource requirement for this activity going forward.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 30/09/2020 - SNOW data has been cleaned.
 30/11/2020 - Policy has been agreed and tools identified.
 30/11/2020 - Missing data for existing assets has been collected.
 01/12/2020 - Implementation of new policy commences.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SECURITY IS COMPROMISED DUE TO INADEQUATE REPORTING, LOGGING AND RESOLVING OF IT SECURITY INCIDENTS/EVENTS

Ref	Sig.	Finding
10		<p>There is no formal information security incident management procedure defining roles, responsibilities and escalation paths resulting from a serious information security incident.</p> <p>Information security could be further compromised as a result of inconsistent and ineffective incident response.</p>

RECOMMENDATION:

A formal incident management procedure should be adopted by the University. This procedure should address roles, responsibilities, time frames for reporting and recovery activities during serious an IT security incident.

MANAGEMENT RESPONSE:

Currently IT security incidents would be managed under the more general IT incident management process. A formal IT security incident management procedure will be adopted at a Group level and tested annually.


A mock-test had been planned for summer 2020 but activities related to Covid-19 have taken priority.

Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 01/01/2021

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LSBU IS NOT ABLE TO RECOVER FOLLOWING A SECURITY INCIDENT - THERE ARE NO MEASURES IN PLACE THAT SUPPORTS RESILIENCY OBJECTIVES

Ref	Sig.	Finding
11		<p>To enable the business processes associated with the end user environment to continue in the event of a disaster, a business continuity plan should be established, supported by contingency arrangements, and tested regularly.</p> <p>An IT Support/Innovation & Transformation Business Continuity Plan was presented to us. This plan has not been formally authorised, but was used as a basis to establish business functionality during the current pandemic crisis. We understand that no serious IT problems were noted during the transformation from office to home based working.</p> <p>However, we noted that no formal organisational recovery plans (e.g. business continuity, disaster recovery) are approved and in place.</p> <p>The absence or ineffective recovery processes and procedures increase the risk that the IT systems or data are not restored in a timely manner following a major disruption.</p>

RECOMMENDATION:

The University should identify and document:

- The most crucial business functions and systems
- The staff and technology resources needed for operations to run optimally
- The time frame within which the functions need to be recovered for CLF to restore operations as close as possible to a normal working state
- The main metric for disaster recovery, the Recovery Time Objective (RTO), Recovery Point Objective (RPO) and the Maximum Tolerable Period of Disruption (MTPD) for the key critical processes

The University should develop Business Continuity and Disaster Recovery Plans as a set of processes to minimise disruption to business services in the event of an outage.

- A BCP and DR awareness and training programme
- IT should test the disaster recovery plan, identify the high risk outcomes and address them
- Based on the new BC and DR Plan, IT should further develop the current incident management practice.

MANAGEMENT RESPONSE:

As noted, an IT Support/Innovation & Transformation Business Continuity Plan is in place but the process to confirm formal authorisation will be clarified with HSR. In light of the recommendation, the plan will be revised to incorporate disaster recovery plans.


Plans will be tested on an annual basis, in parallel with the incident management process.

Responsible Officer:	Graeme Wolfe - Head of IT Security Malvina Gooding - Group Director of IT Services
----------------------	---

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

Implementation 01/01/2021
Date:

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON “NEED TO KNOW” AND “LEAST PRIVILEGE” PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE.

Ref	Sig.	Finding
12		<p>IBM Security Identity Management, which provides centralised identity lifecycle management is implemented at the University.</p> <p>However, the business requirements that specify how access is managed and who may access information and systems under what circumstances are not documented.</p> <p>In addition, we were informed that there is no practice of regular access rights review and that privileged access rights are reviewed on an ad-hoc basis.</p> <p>Failure to control access to data and IT systems to authorised users, processes, or devices increases the risk of data security exposures.</p>

RECOMMENDATION:

Based on business and information security requirements, the University should establish and document an access control policy.

The access control policy should be supported by formal procedures related to:

- A formal user registration and de-registration process
- The provisioning process for assigning or revoking access rights granted to all user types to all systems and services
- Management of privileged access rights
- Review of user access rights.

MANAGEMENT RESPONSE:

A role-based access control project is currently under way and a formal policy will be introduced by 31/12/2020. Currently controls are in place with a named individual within departments needing to authorise permissions which are then enacted by IT Services. These decisions are ad-hoc and not regularly reviewed.

ITrent is in the process of being consolidated at the Group level and will act as the single source of truth for staff data. Access rights will be assigned and revoked based on role, rather than individual. Therefore, staff will not carry forward old permissions when they transfer roles within the Group.

The processes listed in the recommendations will be outlined in the new policy.

Responsible Officer: Malvina Gooding - Group Director of IT Services


LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

Implementation 31/12/2020 - Role-based access policy introduced.
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

DETAILED FINDINGS - SBC

RISK: INFORMATION ASSETS ARE INADEQUATELY SECURED AS A RESULT OF WEAK IT ASSET MANAGEMENT PROCESSES WHICH DO NOT ENSURE THAT IT ASSETS ARE IDENTIFIED, RECORDED, TRACKED AND CLASSIFIED

Ref	Sig.	Finding
13		<p>At Lambeth College, key systems including email and the Distributed File System (DFS) are running on legacy operating systems.</p> <p>At the time of audit there were 45 Windows 2008 servers and five Windows Server 2003 Enterprise Edition on the LSB Lambeth College network.</p> <p>Microsoft ended support for Windows Server 2003 operating system on 14 July 2015 and ended support for Windows 2008 on 14 January 2020.</p> <p>Systems that are not effectively managed and kept up to date will be vulnerable to attacks that may have been preventable.</p>

RECOMMENDATION:

We recommend management put in place a plan to decommission or upgrade these systems.

MANAGEMENT RESPONSE:

There are a range of activities taking place to remediate these risks:


- Email will be moved off local servers by 31/12/2020. 2008 Exchange servers will be replaced with hybrid 2016 solution in the cloud.
- The remaining servers will be assessed for cloud services by 31/12/2020.
- The network replacement will allow for greater connectivity with LSBU and plans in are place to split the LSBU data centre cluster with SBC to improve business continuity for on-premise systems.
- There is a planned consolidation of file system data and then migration to SharePoint online to take advantage of less dependency of on-premise infrastructure and Microsoft security.

Responsible Officer: Malvina Gooding - Group Director of IT Services

Implementation Date: 31/12/2020 - email migration and remaining services assessed.
31/08/2021 - data centre split and half relocated to SBC.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES

Ref	Sig.	Finding
14		<p>To ensure that the network is available when required, the network should be run on robust, reliable hardware and software.</p> <p>We reviewed the Lambeth College network diagram and identified core network devices Cisco 2851 and Cisco 2801 integrated services routers and Cisco Catalyst 4506 and 6509 switches. This network equipment is now obsolete and no longer supported by the supplier.</p> <p>We were informed that there is an action plan to replace the network equipment.</p> <p>Legacy network equipment represents an increased risk of network and IT services being compromised or becoming unavailable in the event of faults.</p>

RECOMMENDATION:

The legacy network equipment should be replaced to ensure that the network is run on vendor supported network devices. The equipment should have security functionality built-in that enables additional security controls to be incorporated easily.

MANAGEMENT RESPONSE:


SBC is included in network replacement programme, as described in Point 2. The SBC network will be addressed in the first phase of deployment in Spring/Summer 2021.

Responsible Officer: Alex Denley, Director of Innovation & transformation and James Rockliffe, Director of Procurement Services (responsible for the successful procurement of the new network technology and service).
Graeme Wolfe - Head of IT Security (responsible for ensuring the network design is secure).

Implementation Date: 01/12/2020 - Tender awarded and new managed service contract begins.
31/03/2021 - Core network redesigned and installation complete

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION COMMUNICATED INTERNALLY/EXTERNALLY IS NOT SUFFICIENTLY PROTECTED RESULTING IN EXPOSURE OF SENSITIVE DATA

Ref	Sig.	Finding
15		<p>As part of the integration process with the University, an external company performed an inventory of the infrastructure and applications at the College.</p> <p>We were informed that besides those inventories there are no processes related to information security asset management.</p> <p>If an asset management process is not in place there is a risk of compromising the confidentiality, integrity and availability of the assets, due to inappropriate identification and protection of assets.</p>

RECOMMENDATION:

IT should:

- Develop a formal asset register which is accurate, up to date, consistent and aligned with other inventories. For each identified asset, ownership of the asset should be assigned.
- Develop a procedure for asset management that will include regular asset reviews.
- Conduct and document an asset-based risk assessment.
- Align implemented security measures with the outcome of the asset-based risk assessment.

These measures could be led at Group level.

MANAGEMENT RESPONSE:


Asset data for SBC does exist but needs to be reviewed for completeness. SBC asset management will be incorporated into the actions identified in Point 9 and managed at a Group level.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 30/11/2020 - Policy has been agreed and tools identified.
30/11/2020 - Missing data for existing assets has been collected.
01/12/2020 - Implementation of new policy commences.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LSBU - LAMBETH COLLEGE IS NOT ABLE TO RECOVER FOLLOWING A SECURITY INCIDENT - THERE ARE NO MEASURES IN PLACE THAT SUPPORTS RESILIENCY OBJECTIVES

Ref	Sig.	Finding
16		<p>The College back-up solution is based on Veeam back-up software. The back-ups are stored locally and there is no off-site backup copy.</p> <p>The current back-up approach is based on weekly full back-ups but without daily incremental back-ups. We were informed that there is no formal evidence of the implemented backup strategy.</p> <p>In addition we noted that regular backup testing is not performed.</p> <p>There is a risk that Lambeth College will be unable to recover the data or recover in time in the event that access to the back-ups is required.</p>

RECOMMENDATION:

Based on business requirements, IT should develop backup documentation, strategy and a technical solution with at least one copy of the backup stored off site. Regular testing of the back-ups should also be introduced.

MANAGEMENT RESPONSE:

As Point 5: A backup policy needs to be developed and implemented at a Group level, as each part of the Group is in a similar position. The college uses a third-party to securely store backup data for a Disaster Recovery scenario.


A backup policy should include live and archive backups.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 30/11/2020 - Backup Strategy has been developed for the Group, with costs identified and approved by the Group Executive.
01/12/2020 - Implementation begins. Duration will be defined by the strategy.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION COMMUNICATED INTERNALLY/EXTERNALLY IS NOT SUFFICIENTLY PROTECTED RESULTING IN EXPOSURE OF SENSITIVE DATA

Ref	Sig.	Finding
17		<p>We reviewed the patch management practice at Lambeth College and noted that there is no formal documentation that describes the requirements for patch management.</p> <p>In addition we were informed that there is a manual process for identifying, acquiring, installing and verifying patches for products and systems. Considering the number of devices in the IT estate, the manual process is inappropriate for consistent and timely application of the security updates.</p> <p>Poor patching can allow malicious software to infect the network and allow security weaknesses to be exploited.</p>

RECOMMENDATION:

Based on the business criticality of the systems, IT should develop a patch management strategy and implement a technical solution for automated patch deployment on devices in the Lambeth College IT estate.

MANAGEMENT RESPONSE:


SBC are covered in the Group patch management policy that has been awaiting approval and will be signed off shortly [see point 6]. A technical solution will be introduced to automate the identifying, acquiring, installing and verifying patches for products and systems.

Responsible Officer: Malvina Gooding, Group Director of IT Services

Implementation Date: 31/08/2020 - Patch management policy approved.
30/09/2020 - New patch management activity commences, and reporting begins.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES

Ref	Sig.	Finding
18		<p>As part of the integration process with the University, penetration testing on a set of external IT addresses at the College network was conducted in January 2020.</p> <p>Weekly vulnerabilities scans on external facing IP addresses are performed along with LSBU.</p> <p>However, whilst details of alerts are passed to the College, we understand there is no formal procedure for addressing these alerts.</p> <p>The lack of a formal procedure for addressing the alerts of penetration tests and vulnerabilities scans increases the risk of non-consistent approach in addressing identified vulnerabilities.</p>

RECOMMENDATION:

A formal procedure for addressing findings identified by penetration testing and vulnerabilities scans should be developed at Lambeth College.

This could be a combined exercise with other parts of the Group.

MANAGEMENT RESPONSE:


SBC will be included in the annual penetration testing that will take place in January across the Group. SBC is currently included in the weekly vulnerability scanning that takes place.

Responsible Officer: Graeme Wolfe - Head of IT Security.

Implementation Date: 31/01/2021

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SECURITY IS COMPROMISED DUE TO INADEQUATE REPORTING, LOGGING AND RESOLVING OF IT SECURITY INCIDENTS/EVENTS

Ref	Sig.	Finding
19		<p>There are no formal information security incident management procedures defining roles, responsibilities and escalation paths resulting from a serious information security incident.</p> <p>Information security could be further compromised as a result of inconsistent and ineffective incident response.</p>

RECOMMENDATION:

A formal incident management procedure should be adopted by the College. This procedure should address roles, responsibilities, time frames for reporting and recovery activities during serious an IT security incident.

MANAGEMENT RESPONSE:


As Point 10: A formal IT security incident management procedure will be adopted at a Group level and tested annually.

Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 01/01/2021

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON “NEED TO KNOW” AND “LEAST PRIVILEGE” PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE.

Ref	Sig.	Finding
20		<p>Code of Practice 7 - Access to Data on College Computerised Administration Systems section of the Lambeth College Information Security policy sets the principles for access to the system and administration of users in the estate. This includes the processes to follow relating to the commissioning and de-commissioning of user access to the systems.</p> <p>However, we were informed that there is no practice of regular access rights review and that privileged access rights are reviewed on an ad-hoc basis.</p> <p>Having active accounts that are no longer required increases the ‘attack surface’ of an organisation which simply means the more accounts there are, the likelihood of an attacker being able to compromise an account increases. It may also lead to unnecessary cost if software licensing is based on active user accounts.</p>

RECOMMENDATION:

IT should perform a regular formal review of accounts used across the College and ensure that accounts not used for a defined period are disabled.

MANAGEMENT RESPONSE:

As part of the Role-Based Access Control project [see point 12], SBC will be implementing improved means of reviewing account status across the non-student accounts. This will be brought in line with LSBU, using ITrent as the source of truth for non-staff accounts.


Student accounts are currently automatically managed based on student enrolment.

Responsible Officer: Malvina Gooding - Group Director of IT Services

Implementation Date: 31/12/2020 - Role-based access policy introduced.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SECURITY IS COMPROMISED DUE TO INADEQUATE REPORTING, LOGGING AND RESOLVING OF IT SECURITY INCIDENTS/EVENTS

Ref	Sig.	Finding
21		<p>Based on the provided equipment inventory, we identified 142 virtual and physical servers at the College. We were informed that there is no antivirus software installed on these servers.</p> <p>Lack of antivirus software on servers increases the risk that information security will be compromised as a result of inadequate protection against malware.</p> <p>We acknowledge that in some instances servers will not require antivirus software and these exceptions should be recorded. It should be noted that the installation of anti-virus software could decrease the server performance on legacy operating systems.</p>

RECOMMENDATION:

The College should install anti-virus software on all servers. We recommend, however, that a risk assessment is undertaken initially to determine if any exceptions to this need to be made. Such exceptions should be documented and approved.

MANAGEMENT RESPONSE:


A review will be undertaken to establish which servers require antivirus and where there are exceptions, these will be documented and reviewed annually.

Responsible Officer: Malvina Gooding - Group Director of IT Services

Implementation Date: 31/12/2020

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SYSTEMS AND INFORMATION ARE INSUFFICIENTLY PROTECTED AS A RESULT OF A LACK OF GOVERNANCE AND ACCOUNTABILITY OVER INFORMATION/ CYBER SECURITY OPERATIONS.

Ref	Sig.	Finding
22		<p>All staff and students in the College should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.</p> <p>Employees of Lambeth College receive an information security awareness training as part of induction, but there is no further information security training.</p> <p>Failure to provide the College personnel with information security awareness training increase the risk of personnel being unable to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>

RECOMMENDATION:

The College should establish an information security awareness training programme in line with information security policies and relevant procedures.

The information security awareness training programme should take into consideration the data to be protected and the controls that have been implemented to protect the data.

The awareness programme should be planned taking into consideration the roles in the College, and, where relevant, the College expectation of the security awareness of external contractors.

This training could be developed and managed at Group level to avoid duplication of effort.

MANAGEMENT RESPONSE:

Complete: Following COVID-19 period of disruption and rapid move to work-from-home scenario the college has now released online training module as a mandatory requirement for staff to raise awareness on cyber security.


Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 30/09/2020

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

DETAILED FINDINGS - SBA

RISK: SYSTEMS AND INFORMATION ARE INSUFFICIENTLY PROTECTED AS A RESULT OF A LACK OF GOVERNANCE AND ACCOUNTABILITY OVER INFORMATION/ CYBER SECURITY OPERATIONS.

Ref	Sig.	Finding
23		<p>We identified 681 active directory (AD) accounts that had passwords set never to expire and 897 AD accounts with password not required settings. In addition we also identified accounts that had not logged in since 2014, 2015, 2016, 2017 and 2018.</p> <p>Not requiring passwords and having never expiring passwords increases the likelihood that an account will be compromised (guessed, stolen or cracked). In addition, if the account is not used and is compromised the attackers' access will continue indefinitely.</p> <p>Having active accounts that are no longer required increases the 'attack surface' of an organisation which simply means the more accounts there are, the likelihood of an attacker being able to compromise an account increases.</p>

RECOMMENDATION:

We recommend that the SBA performs a regular formal review of accounts used and ensure that passwords are used according the formal password policy. Any accounts not used for a defined period should be disabled.

MANAGEMENT RESPONSE:

SBA does not have a formal password policy. LSBU's password policy has not been formally approved so will be revised to incorporate all institutions within the Group and signed off by the Group Executive.

Old accounts identified in the audit relate to ex-students and should have been archived. These will be disabled with immediate effect. They are usually reviewed every September but some have clearly been missed.


Many teachers are currently working remotely and connecting via the VPN. When staff return to SBA buildings in early September, password rules will be changed to force an immediate password reset and passwords will expire every 180 days from that date.

Responsible Officer:	Password Policy approval - Alison Chojna, Acting Executive Director of Academic Related Resources. Password rule changes and archiving - Ewaen Igbinovia, Service Manager (Pallant Managed Services)
----------------------	---

Implementation Date:	11/09/2020 - Password policy approved. 18/09/2020 - Password complexity introduced and archiving complete.
----------------------	---

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES.

Ref	Sig.	Finding
24		<p>The network implementation in both academies is based on two core switches that provide a backbone for the network. We were informed that the current capacity of the backbone is unable to cope with the current levels of traffic and security exposure.</p> <p>If the current design is not improved there is a risk of issues relating to network and IT services availability.</p>

RECOMMENDATION:

SBA should work with the outsourced provider to assess the reported current capacity issues. This could include:

- Arranging fall-back to alternative points of connection and links
- Providing duplicate or alternative points of connection to communications carriers.

MANAGEMENT RESPONSE:

UAE employed a network consultant over the summer to assess the current capacity. Core switches are in good condition but edge switches need replacing. New hardware has arrived and will be deployed in August 2020. Segmentation, configuration and optimisation is currently being worked on. UAE are moving towards a one device per user strategy for staff and students. The works undertaken this summer will provide the capacity to enable that strategy. IP addresses are private.


UTC is a small building and currently capacity is adequate to meet the needs. A network assessment has not been undertaken at UTC but will be considered in the future.

Responsible Officer: Ewaen Igbinovia - Service Manager (Pallant Managed Services)

Implementation Date: 29/08/2020 - upgrades, segmentation and optimisation of UAE network.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES.

Ref	Sig.	Finding
25		<p>There is an annual device audit that inventories the laptops desktops and phones, but there are no inventories related to IT infrastructure and applications in use.</p> <p>If there is not a complete asset management process in place, there is a risk of compromising the confidentiality, integrity and availability of the assets, due to an inappropriate identification and protection of assets.</p>

RECOMMENDATION:

SBA should:

- Develop a formal asset register which is accurate, up to date, consistent and aligned with other inventories. For each identified asset, ownership of the asset should be assigned.
- Develop a procedure for asset management that will include regular asset reviews.
- Conduct and document an asset-based risk assessment.
- Align implemented security measures with the outcome of the asset-based risk assessment.

This process could be managed at Group level.

MANAGEMENT RESPONSE:

SBA does have the capability to track assets, including software, and an annual audit is undertaken. However, there is not a single pane of glass over all the assets and the information is located in multiple systems.


An asset management process will be adopted at a Group level [see point 9] moving towards a single source of truth for all Group IT assets. A Group level role will be created to oversee this activity.

Responsible Officer: Malvina Gooding - Group Director of IT Services

Implementation Date: 30/11/2020 - Policy has been agreed and tools identified.
30/11/2020 - Missing data for existing assets has been collected.
01/12/2020 - Implementation of new policy commences.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LSBU - ACADEMIES IS NOT ABLE TO RECOVER FOLLOWING A SECURITY INCIDENT - THERE ARE NO MEASURES IN PLACE THAT SUPPORTS RESILIENCY OBJECTIVES

Ref	Sig.	Finding
26		<p>The outsource provider, Pallant Managed Services Ltd, is responsible for the backup process in both academies. The backups are stored locally on network attached storage. There is no off-site copy of the backups or evidence of the implemented backup strategy.</p> <p>In addition we noted that regular backup testing is not performed.</p> <p>There is a risk that the academies will be unable to recover the data or recover in time in the event that access to the backups are required.</p>

RECOMMENDATION:

Based on academies' business requirements, Pallant Managed Services should develop backup documentation, strategy and a technical solution with at least one copy of backup stored off site. Regular testing of the backup should also be introduced.

MANAGEMENT RESPONSE:

A plan is currently being developed and costed to moved towards full off-site back-up on a weekly basis. Plan one week full back-up to off-site location. Need to put the numbers together.


SBA will be folded into the Group Backup Strategy when agreed, to support a single way of working across the Group.

Responsible Officer:	SBA local solution - Ewaen Igbinovia, Service Manager (Pallant Managed Services) Development and implementation of Group back-up policy - Malvina Gooding, Group Director of IT Services
----------------------	---

Implementation Date:	30/09/2020 - SBA interim local solution 30/11/2020 - Backup Strategy has been developed for the Group, with costs identified and approved by the Group Executive. 01/12/2020 - Implementation begins. Duration will be defined by the strategy.
----------------------	---

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: INFORMATION AND/OR IT INFRASTRUCTURE IS EXPOSED DUE TO UNDEFINED AND IMPLEMENTED IT AND NETWORK PROTECTION, RECOVERY RESPONSIBILITIES AND RISK MITIGATION MEASURES.

Ref	Sig.	Finding
27		<p>There is no history of regular penetration test and vulnerability scans at either of the academies' infrastructure.</p> <p>Lack of regular penetration testing and vulnerability assessments increases the risk of vulnerabilities going undetected.</p>

RECOMMENDATION:

Regular penetration testing and vulnerability scans should be implemented at least annually and upon significant changes. This will need to be negotiated with the outsource provider.

MANAGEMENT RESPONSE:


Currently vulnerability scans are taking place on an ad hoc basis using a free tool. LSBU to extend vulnerability scanning software to cover SBA and scan on a weekly basis. SBA to be included in annual penetration testing undertaken by an external provider.

Responsible Officer: Graeme Wolfe - Head of IT Security.

Implementation Date: 30/09/2020 - Vulnerability scans to commence at SBA.
31/01/2021 - SBA to be included in annual penetration testing.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SYSTEMS AND INFORMATION ARE INSUFFICIENTLY PROTECTED AS A RESULT OF A LACK OF GOVERNANCE AND ACCOUNTABILITY OVER INFORMATION/ CYBER SECURITY OPERATIONS.

Ref	Sig.	Finding
28		<p>Information security policies provide the management direction and support information security in accordance with business requirements and relevant laws and regulations.</p> <p>We noted that South Bank University Engineering (UTC) does not have an information security policy.</p> <p>This increases the risk that an inappropriate set of security controls is implemented at UTC.</p>

RECOMMENDATION:

A comprehensive, documented information security policy should be produced by UTC and communicated to all individuals with access to UTC's information and systems.

Assistance from the Group management could be sought for this process.

MANAGEMENT RESPONSE:


LSBU to share existing information security policy with the UTC. To be approved by SBA governing body. Longer-term a Group-wide information security policy should be adopted where appropriate.

Responsible Officer: Graeme Wolfe - Head of IT Security.

Implementation Date: 31/10/2020 - UTC approved the SBA information security policy.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON “NEED TO KNOW” AND “LEAST PRIVILEGE” PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE.

Ref	Sig.	Finding
29		<p>At the academies, the management of access rights and permissions is the responsibility of Pallant Managed Services.</p> <p>We identified that the business requirements for deciding how access is managed and who may access information and systems under what circumstances is not established and documented.</p> <p>In addition, we were informed that there is no practice of regular access rights review and that privileged access rights are reviewed on an ad-hoc basis.</p> <p>Failure to control access to data and IT systems to authorised users, processes or devices increases the risk of data security exposures.</p>

RECOMMENDATION:

Based on business and information security requirements, the academies should establish and document an access control policy. The purpose of this policy is to ensure that both logical and physical access to data and systems is controlled and procedures are in place to ensure the protection of information systems and data.

The access control policy should be supported by formal procedures related to:

- A formal user registration and de-registration process
- The provisioning process for assigning or revoking access rights granted to all user types to all systems and services
- Management of privileged access rights
- Review of user access rights.

MANAGEMENT RESPONSE:

A full review is to be completed of SBA by end October 2020. As identified, currently access rights are approved on an ad-hoc basis and are not regularly reviewed.


SBA to be incorporated into the Group role-based access control project that is currently underway [see point 12]. A formal access control policy will be adopted and procedures agreed.

Responsible Officer:	Full review completed - Ewaen Igbinovia, Service Manager (Pallant Managed Services) Access control policy and procedures developed - Malvina Gooding, Group Director of IT Services
----------------------	--

Implementation Date:	31/10/2020 - initial review complete. 31/12/2020 - Role-based access policy introduced.
----------------------	--

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: LOGICAL AND PHYSICAL ACCESS TO INFORMATION AND INFORMATION PROCESSING FACILITIES ARE NOT LIMITED BASED ON “NEED TO KNOW” AND “LEAST PRIVILEGE” PRINCIPLES RESULTING IN UNAUTHORISED ACCESS TO INFORMATION AND/OR IT INFRASTRUCTURE

Ref	Sig.	Finding
30		<p>We were informed that the access to the server room is not restricted at South Bank University Engineering (UTC).</p> <p>We were unable to verify this as the audit was performed remotely.</p> <p>This increases the risk of unauthorised physical access, damage and interference to UTC’s data and data processing facilities.</p>

RECOMMENDATION:

UTC should protect the server room by appropriate entry controls to ensure that only authorised personnel are allowed access.

Access rights to server rooms should be regularly reviewed and updated, and revoked when necessary.

MANAGEMENT RESPONSE:

Currently access is possible for anyone with a master key.


Additional entry controls will be introduced, limiting access to IT and Estates staff only.

Responsible Officer: Ewaen Igbinoia, Service Manager (Pallant Managed Services)

Implementation Date: 30/09/2020

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

RISK: SYSTEMS AND INFORMATION ARE INSUFFICIENTLY PROTECTED AS A RESULT OF A LACK OF GOVERNANCE AND ACCOUNTABILITY OVER INFORMATION/ CYBER SECURITY OPERATIONS.

Ref	Sig.	Finding
31		<p>All employees in the academies should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.</p> <p>Employees of the academies receive information security awareness training during the induction process, but there is no further information security training.</p> <p>Failure to provide academy personnel with information security awareness training increases the risk of personnel being unable to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>

RECOMMENDATION:

The academies should establish an information security awareness training programme in line with information security policies and relevant procedures.

The information security awareness training programme should take into consideration the data to be protected and the controls that have been implemented to protect the data.

The process could be developed and managed at Group level to avoid duplication of effort.

MANAGEMENT RESPONSE:

Mandatory online cyber security training is in place at LSBU and will be extended to include all institutions in the Group.

Responsible Officer: Graeme Wolfe - Head of IT Security

Implementation Date: 30/09/2020

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

OBSERVATIONS - LSBU

LACK OF NETWORK LOGICAL NETWORK DIAGRAMS

There is a lack of L3 (Layer 3) logical network diagrams.

Good L3 diagrams consist of the following information: Subnets (VLAN IDs, names, network address and subnet mask), L3 Devices (at least routers, firewalls, VPN devices, most important servers as DNS servers, their IP addresses, logical interfaces) and routing protocol information.

L3 diagrams are vital for troubleshooting or for planning changes.

It is noted that LSBU provided additional documentation related to the network configuration.

END-OF-LIFE DESKTOP OPERATING SYSTEM IN THE IT ENVIRONMENT

At the time of audit there were Windows 7 computers on the LSBU network. The IT department was updating and reviewing the accuracy of Snow (the tool used to identify out of date machines) and therefore we were unable to determine the exact number of machines there are in place.

On 14 January 2020, Microsoft stopped supporting Windows 7 meaning that security updates will no longer be released and these devices will therefore present an increased risk to LSBU systems.

It is noted that a plan to decommission or upgrade these systems has been put in place. There are plans to complete this by the end of 2020. However, these machines are not being used a present.

OBSERVATIONS - SBA

NO REPORTING AND SECURITY METRICS ASSOCIATED WITH THE PATCH MANAGEMENT

Pallant Managed Services Ltd is responsible for the patch management practice in both academies.

High level requirements related to the patch management are defined in the managed service contract between the academies and Pallant Managed Services Ltd.

It would be good practice if reporting on patch management be introduced as a regular monthly intervals.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY





STAFF INTERVIEWED

BDO LLP APPRECIATES THE TIME PROVIDED BY ALL THE INDIVIDUALS INVOLVED IN THIS REVIEW AND WOULD LIKE TO THANK THEM FOR THEIR ASSISTANCE AND COOPERATION.




Malvina Gooding	Group Director of IT Services
Graeme Wolfe	Head of Information Security
Adam Bird	IT Services Manager & ProMonitor Support
Sarah Oyet	Head of Applications and Infrastructure
Sarah Kuria	Trust Administration Officer
Dan Cundy	Executive Principal
Ewaen Igbinoia	Service Manager (Pallant Managed Services)
Steven Knott	Pallant Managed Services
Felipe Lima	Pallant Managed Services
Ayo Alalade	UAE
Fiona Brown	UTC

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

APPENDIX I - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN OF INTERNAL CONTROL FRAMEWORK		OPERATIONAL EFFECTIVENESS OF CONTROLS	
	FINDINGS FROM REVIEW	DESIGN OPINION	FINDINGS FROM REVIEW	EFFECTIVENESS OPINION
Substantial 	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited 	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

RECOMMENDATION SIGNIFICANCE

High 	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

APPENDIX II - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The purpose of the audit is to provide assurance on the adequacy and effectiveness of information security at the LSBU Group.

KEY RISKS:

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding the key risks associated with the area under review are:

- Systems and information are insufficiently protected as a result of a lack of governance and accountability over information/ cyber security operations
- Information and/or IT infrastructure is exposed due to undefined and implemented IT and network protection, recovery responsibilities and risk mitigation measures
- Logical and physical access to information and information processing facilities are not limited based on “need to know” and “least privilege” principles resulting in unauthorised access to information and/or IT infrastructure
- Information communicated internally/externally is not sufficiently protected resulting in exposure of sensitive data
- Information assets are inadequately secured as a result of weak IT asset management processes which do not ensure that IT assets are identified, recorded, tracked and classified
- Security is compromised due to inadequate reporting, logging and resolving of IT security incidents/events
- The Group entities are not able to recover following a security incident - there are no measures in place that supports resiliency objectives.

LONDON SOUTH BANK UNIVERSITY GROUP, INFORMATION SECURITY

SCOPE OF REVIEW:

For the university, College and Academies the review will consider:

- **Identify** - Information security policies, standards procedures and strategies, as well as risk assessment processes, cyber threat intelligence gathering, security governance and training / awareness.
- **Protect** - Design of the network (isolation and segmentation), as well as the management of key controls such as perimeter (firewall) configuration, access restrictions, asset management (including mobile assets) and cryptograph.
- **Detect** - Threat detection controls, such as for intruder detection systems and antivirus/malware tools.
- **Respond** - Security event and incidents management processes.
- **Recover** - Data backup/restore, fail-over and recovery processes.

As part of the Protect section, we will identify the information security perimeter and the information entry and exit points (IT and non-IT based). We will then consider the corresponding controls in place to manage threats, and the risks of data leakage at each point. This will support us in identifying control gaps and infrastructure components that are vulnerable to attack.

As part of the Recover section, we will consider new disaster recovery plans, facilities and systems, and a) the protection afforded to the data held within them and b) the effectiveness of the recovery measures in supporting continuity after a cyber-attack.

In addition, Internal Audit will bring to the attention of management any points relating to other areas that come to their attention during the course of the audit. We assume for the purposes of estimating the number of days of audit work that there is one control environment for each entity, and that we will be providing assurance over controls in this environment. If this is not the case, our estimate of audit days may not be accurate.

APPROACH:

We will consider the information/cyber security controls in alignment with the (US) National Institute of Standards and Technology (NIST) cyber security framework, with additional controls identified within the Cyber Security Nexus (CSX) framework from the IS Audit and Control Association (ISACA).

Our approach will be to conduct interviews to establish the controls in operation for each of our areas of audit work. We will then seek documentary evidence that these controls are designed as described. We will evaluate these controls to identify whether they adequately address the risks.

We will seek to gain evidence of the satisfactory operation of the controls to verify the effectiveness of the control through use of a range of tools and techniques.

FOR MORE INFORMATION:

RUTH IRELAND

+44 (0)20 7893 2337
ruth.ireland@bdo.co.uk

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright ©2020 BDO LLP. All rights reserved.

www.bdo.co.uk

This page is intentionally left blank