

Meeting of the Group Audit and Risk Committee

5.00 pm on Thursday, 28 October 2021
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.	Cyber incident review	3 - 10	NL
4.	IT disaster recovery internal audit report (draft)	11 - 40	NL
5.	Cloud migration: fact finding and lessons learned	41 - 48	NL

Date of next meeting

3.30 pm on Thursday, 11 November 2021

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

In attendance: David Phoenix, Natalie Ferer, Richard Flatman, Kerry Johnson, Stuart Johnston, Nicole Louis and James Stevenson

Internal auditors: Ruth Ireland and Gemma Wright (BDO)

This page is intentionally left blank

Agenda Item 3

	CONFIDENTIAL - RESTRICTED TO MEETING PARTICIPANTS
Paper title:	Cyber Incident Review by Group Director IT
Board/Committee:	Group Audit and Risk Committee
Date of meeting:	28 October 2021
Author(s):	Stuart Johnston, Group Director of IT
Sponsor(s):	Nicole Louis, Chief Customer Officer – LSBU Group
Purpose:	For Discussion
Recommendation:	The Committee is requested to discuss the recovery actions, issues and lessons learned from the December 2020 cyber incident.

Executive summary

LSBU experienced a Ransomware attack around 12 December 2020 with virtual machine files being compromised and encrypted which effecting denied access to all on-campus hosted services. Cyberclan, an external cyber security consulting group, assisted LSBU with the incident and has confirmed that whilst there was evidence of system access during the attack, that there was no evidence of data exfiltration found.

This attack occurred whilst student and staff were already affected by Covid19 and the loss of core applications significantly impacted on the student and staff experience for an extended period of time. Teaching systems were prioritised and begun to be recovered late January 2021 with services being progressively recovered into Summer 2021.

This paper provides the recovery actions and improvements completed during the recovery phase and identifies lessons learnt that will inform the IT department roadmap and LSBU business planning process. These lessons may be categorised into two broad themes that highlight systemic failures in IT leadership, organisational capability development and investment over multiple years:

- Low IT operational maturity around people, process, and technology
- Technology Capability Gap

Some of these lessons overlap with recommendations identified in the BDO IT Security Audit (August 2020) and the IT Disaster Recover Audit (September 2021) as well as the work underway to achieve Cyber Essentials accreditation.

LSBU Cyber Incident December 2020 Review by Group Director IT

Incident Summary

1. LSBU experienced a Ransomware attack around 12 December 2020 with 547 virtual machine files being compromised which effecting denied access to all on-campus hosted services.
2. CyberClan, a specialist cyber security group, were engaged to assist with our recovery from this attack from a variant of HelloKitty. Cyberclan's report has confirmed, that, based on their review of the forensic data obtained, that whilst there was evidence of system access during the attack, that there was no evidence of data exfiltration found.
3. In consultation with CyberClan the University decided that rather than restoring services and applications to their previous conditions that we would take a zero-trust approach as were unable to confirm if any 'hooks' had been left in our systems. All systems were double scrubbed, and then the majority were upgraded and patched to the latest security levels before restoration. Role-based access to systems was enforced to ensure only users that require access have the relevant permissions, including IT staff. The core network and associated services were re-engineered, a new virtual private network setup and all devices moved to new network addresses. This remediation work has resolved some of the underlying, historical issues and technical debt which reduces our risk of another attack and will speed up the recovery from any future cyber incident. Several areas have been identified in the lessons learnt that will require leadership, operational improvements, and ongoing investment to further improve our overall cyber security assurance levels.
4. This substantive remediation approach improved the security of our systems but considerably extended the recovery time and associated impact on customers, with services being progressively restored over eight months.
5. On recognising the attack the Universities Incident Response was triggered and Gold Command unit set up. Restoration of services was prioritised by Gold Command with services such as telephony, Moodle, Panopto and Library resources being prioritised and available by late January 2021 and most core services recovered by May 2021. The remaining services were then progressively restored with the last major services only restored by clearing and enrolment in Summer 2021.
6. This cyber incident has had a significant impact on the core business and reputation of the University at a time when students and staff were already grappling with Covid19. School and Professional Services staff have worked extraordinarily hard and patiently to develop manual workarounds to continue to support students and staff through this period. SBC was also directly impacted as they rely on the group Finance (Agresso) and HR (iTrent) applications to support business. This incident also significantly impacted on the delivery of LEAP and other change initiatives across the University. BDO IT Security audit recommendations have also been delayed as staff have been fully committed to recovery activities.

Recovery Actions and Associated Issues

Recovery Resources

7. IT staff have risen to the operational challenge and have worked extremely hard over this recovery phase to re-engineer and recover services as quickly as possible.

8. A Network Infrastructure Lead role was created and recruited in March 2021 to operationally improve how our network service provider interacts with our other IT teams.
9. Additional contracted resources were added to the IT department to add both capacity and specialist knowledge to support the recovery programme of work. These resources worked well with standard services but were less effective with some of our more complex or heavily customised services.
10. **Suppliers and managed service partners.** Support and development for many key services and applications are outsourced either through managed service contracts or purchased service/development days. Whilst some suppliers have been able to respond quickly, others have required lead times of several weeks, have not been able to scale for the additional staff resources needs or in the case of ISIM (the user management interface developed as part of the work with IMB), have failed to deliver the service needed.
11. **Predicting timescales.** External advice from third parties such as JISC and other universities was used to triangulate and check information being provided on likely timescales. Establishing accurate timeframes though has been very challenging due to the complexity of each restoration, the interdependencies and reliance on third parties and limited documentation of existing services. The priority order was communicated and reviewed at the fortnightly Recovery Operations Group meeting, attended by Schools and Heads of Services. However, timeframes have had to be refreshed several times and this has proved a source of frustration to staff and students.
12. **BAU and projects.** As the restoration has progressed, BAU activities have been re-established and major projects, such as LEAP and the Campus Development Programme, needed to be supported in parallel to restoration activities. This has been challenging to manage and resource across these competing requirements.

Process

13. **IT Security Governance.** A Group IT Security and Resilience Board (ISRB) was initiated in October 2020 to provide oversight of security and resilience work, track key performance indicators, and ensure that internal audit recommendations are actioned. The board is co-chaired by James Stevenson and Nicole Louis.
14. **IT Security Operations Group.** A new group was setup in August 2021 that draws from staff across the IT department to raise security awareness, identify gaps and develop best practices to deliver on the agreed IT roadmap. This monthly meeting is chaired by the Group Head of Information Security.
15. **Patching.** At the time of the incident IT did not have a regular, monthly patching process in place to ensure infrastructure and computers received critical security patches. IT now has introduced a monthly patch process for PCs, Laptops, Macs and Servers. Further work will be undertaken improve the patch reporting service and to reduce the hazard window caused by this monthly patching.
16. **Jisc Gold builds.** Jisc is used to test our desktop/laptop and server “Gold” images to ensure that these build templates are appropriately hardened.
17. **Vulnerability Scanning.** Outside of annual Jisc penetration testing IT has implemented external vulnerability scanning solution (E2E) that scans and reports on core public facing services to identify security vulnerabilities on a weekly basis.

Technology

18. As part of the recovery actions several underlying technology improvements have already been implemented to improve the ongoing IT security capability of LSBU.
19. **Server and application infrastructure recovery.** The server restoration process revealed that 47% of servers were running non-compliant operating systems. As services were scrubbed and restored IT has upgraded and patched the underlying infrastructure and applications to the latest versions. This upgrade process has substantially improved our security stance but did add to the cost and time to recover services.
20. Where practical IT also worked with vendors to re-engineer and simplify the underlying services with overall number of Virtual Machines being reduced down from 547 to 478 production servers.
21. There are still 68 servers (14%) that were not able to be updated as part of the recovery, for example if the application was not able to be upgraded at that point in time. These legacy services are operating in a restricted mode until IT and business stakeholders can schedule them to be replaced or upgraded. For example, myLSBU is currently running on a legacy Redhat version to allow exam results to be published and will be upgraded 9 October 2021.
22. IT also introduced more comprehensive and secure Privileged Account Management (PAM) that are used to access and move data around our services.
23. **Back-up service.** The backup solution was previously on-campus only. Prior to the cyber incident a new backup solution had been scoped to bring LSBU in line with current best practice. This new service has been implemented as a managed service using Veeam technology and includes both on-site 14 day retention of backups as well as daily off-site replication to a Zadara private cloud based storage service has been implemented.
24. **Desktop and laptop recovery.** At the time of the incident LSBU was operating a large number of Windows 7 PCs that were end of life in January 2020. As part of the recovery IT upgraded all of these devices to a supported version of Windows 10 Enterprise edition.
25. **Anti-virus and security monitoring.** LSBU has replaced it's older software with a next generation anti-virus solution (Sophos Intercept X) which also provides a 24/7 security operations centre (SOC), which monitors for threats and proactively blocks any suspicious activity.
26. The perimeter vulnerability scanning solution (E2E) has also been extended to monitor more of LSBU services and has also been extended to key SBC and SBA services. This external service scans for security vulnerabilities in our internet or public facing services to proactively alert IT staff of areas to improve.
27. **Network replacement.** Prior to the incident the Major Project Investment Committee (MPIC) had already approved funds to undertake the Phase 1 of a complete redesign and replacement of LSBU's network. This work had already identified the need to move to a more advanced network solution including new firewalls, virtual private network and move to network segmentation.
28. The modern network design that had begun to be developed as part of the Network Replacement project was accelerated and new firewalls, virtual private network, domain name servers and the core network have been replaced at Southwark. The new, segmented design has been implemented which will limit any future breaches from spreading across our network. This change in the design substantially improves our cyber security stance but meant that every device on the network had to move to a new address with new, improved firewall rules which did substantially impact on the recovery timeline.

Lessons Learnt

29. The following key lessons learnt will need to be developed into the IT Departmental Roadmap and into the overall business planning process. Overall, the key lessons may be categorised into two broad themes that highlight systemic failures in IT leadership, organisational capability development and investment over multiple years:
- Low IT operational maturity around people, process and technology
 - Technology Capability Gap
30. Some of these lessons learnt overlap with recommendations identified in the BDO IT Security Audit (August 2020) and the IT Disaster Recover Audit (September 2021) as well as the work underway to achieve Cyber Essentials accreditation.

IT Operational Maturity

31. The following lessons learnt focus on those that directly link to the cyber incident but are, by their nature, part of the broader capability and capacity improvement work that IT needs to undertake.
- a) IT staff skills. IT does not consistently invest in technical skills to ensure staff have the appropriate capabilities to maintain and develop IT services to meet business requirements. Additional Opex has been identified and allocated for this FY to begin to remediate this oversight.
 - b) IT structure. IT will review the overall structure and resource allocation within our current budget to identify opportunities to improve productivity and refocus FTE on technology and process improvements. This change initiative will need to be managed around other commitments with a formal submission planned this academic year.
 - c) Vendor/External managed services. IT will develop more strategic relationships with key vendors and suppliers to ensure that we are able to source additional resources to support major incidents impacting on key business services.
 - d) Documentation. All internal and external services provided by IT should have detailed support documentation (service design, support model and data flows) to allow IT to quickly diagnose and restore services. We will work with other departments and schools to document the underlying IT services required by their independently managed solutions.
 - e) IT Disaster Recovery Plan. IT does not have an IT DR plan and will need to engage an external consultant to help them develop an appropriate framework, including:
 - Roles and responsibilities for IT DR and data backups, including an assessment of key person dependencies and commitment from senior management.
 - ITDR policies, plans and procedures.
 - IT DR testing and training.
 - f) Post recovery testing. LSBU does not have a clear set of roles and procedures around regression testing of services when they have been restored. Depending on the service this may range from a short list of manual test cases through to automated testing tools to confirm that critical business processes are operating correctly.
 - g) Review operating boundary between EAE and IT. The current operational support responsibilities between EAE and IT should be reviewed to establish if the end-to-end support processes can be made more efficient. For example, to setup a computer on a desk currently requires EAE to physically patch from the switch to the wall socket and then IT to configure the switch.

32. IT needs to develop a clear technology refresh roadmap with associated investment to ensure that the current services are maintained appropriately to minimise the level of technical debt across LSBU. This will reduce the risk of future cyber incidents and will improve the speed of service recovery.
- a) Desktop/Laptop operating systems. IT to move to annually updating student and staff computers to current operating systems. This will include identifying and replacing equipment that is no longer able to be upgraded as part of a rolling, equipment replacement programme.
 - b) Application and Server Upgrades. IT will coordinate with business service owners to ensure funding and time is allocated to allow for applications to be upgraded at least once per year where possible. Where services are not able to be upgraded then replacement programs will be developed. New versions of applications not only have improved security patching but are also more readily supported by external support companies.

Technology Capability Gaps

33. IT will need to develop a programme to address the following service capability gaps:
- c) Group Data Centre resilience. LSBU and the Group does not have an appropriately resilient data centre capability with single points of failure within the current infrastructure. IT has developed a strategy to relocate existing equipment from Southwark to an existing room in Clapham to provide a shared, resilient Group service in 2022 as a temporary solution. The new Vauxhall site is being investigated as the long-term solution to ensure core infrastructure services are resilient and support DR objectives across the group.
 - d) Cloud Adoption. Only a limited number of services are currently hosted on the cloud. IT needs to prioritise and deliver on the existing strategy to relocate services to Software as a Service (SaaS) or cloud based managed services where available and commercially viable. This will reduce the on-campus infrastructure requirements whilst exploiting the resilience native to cloud based services.
 - e) Data Integration. The Integration Platform project will introduce a modern, integration platform (Boomi) that will replace the complex and fragile point to point data integrations that share data between our services. This project has just started and will run through to SRS go-live in December 2022.
 - f) Identity and Access Management (IAM). The current solution (ISIM) is no longer fit for purpose, is overly complex and requires skills that are not widely available in the market. IT will look to replace the current solution (ISAM) with a simpler and cheaper to maintain solution in FY2022/23. IT will introduce Multi-Factor Authentication (MFA) via our Microsoft technology stack in FY2021/22.
 - g) Solution Complexity. LSBU operates several services that are underpinned by bespoke, overly fragile or complex solutions that have higher support and recovery overheads. Against the 2025 strategy the University has begun to invest in a digital transformation programme that will simplify and modernise these solutions which will further mitigate the cyber security risks and time taken to recover services in the future. For example, the LEAP SRS project will dramatically reduce the number of legacy services required to support this critical student administrative system.
 - h) Remote Access. Currently over 800 staff remotely connect to their desktop PC in the office to allow them access key business applications. This type of is not robust and significantly delayed the recovery of services as staff needed to be setup to securely work from both

their laptops and their 'legacy' desktop computer. IT will look to deploy a Desktop as a Service (DaaS) solution to provide a more flexible and secure offering to staff.

- i) Improved laptop and desktop computer management. IT will further refine and introduce improved end device tools (InTune/End Point Configuration Manager/Jamf) and asset management to further secure and operationally manage student and staff computers.
- j) Monitoring and Alert. IT has already implemented Sophos Managed Threat Response service which pro-actively monitors, acts and alerts LSBU in the event of an issue. IT will investigate and recommend if we should evolve our monitoring and alert services which may include a broader Security and Incident Event Monitoring (SIEM) or other advanced data protection services as part of the group security roadmap.

This page is intentionally left blank

	INTERNAL
Paper title:	LSBU IT Disaster Recovery Audit
Board/Committee:	Group Audit and Risk Committee
Date of meeting:	28 October 2021
Author(s):	Stuart Johnston, Group Director of IT
Sponsor(s):	Nicole Louis, Chief Customer Officer
Purpose:	For Discussion
Recommendation:	The Committee is requested to discuss the initial response to the draft BDO IT disaster recovery audit.

Executive summary

An audit of the Group's IT Disaster Recovery (DR) arrangements was undertaken as part of the 2020/21 Internal Audit Plan for the group. The audit covers London South Bank University, Lambeth College and South Bank Academies. The purpose of the audit is to provide assurance over the design and operational effectiveness of IT DR policies and procedures in place at the LSBU Group.

The information collection was undertaken in June 2021 and the draft report was delayed and was issued on 3 September 2021. Management responses have not yet been provided to the BDO.

Overall, the BDO report has identified substantial gaps in our design and operational procedures to mitigate the risks associated with the loss of our key IT services. BDO have documented nine findings; four of high significance, four of medium significance and one of low significance.

	LEVEL OF ASSURANCE	
	Design	Operational Effectiveness
LSBU	No	Limited
SBC	Limited	Limited
SBA	Moderate	Limited

This extremely poor level of assurance reflects the current low level of IT maturity across the group. IT leadership will need time to develop a comprehensive disaster recovery plan which addresses the findings in the report in a way which results in embedded and sustainable practice. The plan will need adequate resourcing and funding to enable us to substantially improve our people, processes and technology and in doing so, address this systemic and long standing issue. IT requests that we are given until the next GARC meeting to develop a funded and achievable remediation which is first properly considered with the Group Executive, particularly if there are funding implications. This programme of remediation will include:

- DR Plan and Procedures: To enable us to move at pace, whilst continuing to deal with a substantial number of IT operational priorities, IT leadership will engage an external company to assist the group to develop and deliver against the key gaps identified in this audit including:
 - Business Impact Assessment and development of DR metrics
 - DR Plan with clear roles and responsibilities identified
 - Document and improve procedures and communication process
 - Link the IT DR Plan with the Groups Business Continuity Plans (BCP)
- Data Centre/Core network: The audit identifies that we do not have an alternative service provision to maintain operations in the event of a physical site failure. IT has developed a strategy to relocate existing equipment from Southwark to an existing room in Clapham to provide a shared, resilient Group service in 2022 as a temporary solution. The new Vauxhall site is being investigated as the long-term solution to ensure core infrastructure services are resilient and support DR objectives across the group.

This infrastructure work is being done alongside our adoption of cloud-based services as per our agreed strategy.

The response and tracking of remediation actions to this audit will be overseen by the Group IT Security and Resilience Board, co-chaired by James Stevenson and Nicole Louis.

LONDON SOUTH BANK UNIVERSITY GROUP

INTERNAL AUDIT REPORT - DRAFT

IT DISASTER RECOVERY
SEPTEMBER 2021

	LEVEL OF ASSURANCE	
	Design	Operational Effectiveness
LSBU	No	Limited
SBC	Limited	Limited
SBA	Moderate	Limited



LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

EXECUTIVE SUMMARY	2
DETAILED FINDINGS - GROUP	8
DETAILED FINDINGS - LSBU.....	10
DETAILED FINDINGS - SBC	16
DETAILED FINDINGS - SBA	20
STAFF INTERVIEWED	23
APPENDIX I - DEFINITIONS.....	24
APPENDIX II - TERMS OF REFERENCE	25

DISTRIBUTION

Stuart Johnston	Group Director of IT & Digital Transformation
Malvina Gooding	Group Director of IT Services
Adam Bird	IT Services Manager & ProMonitor Support - Lambeth College
Dan Cundy	Executive Principal, South Bank Academies

REPORT STATUS LIST







Auditor:	Goran Bonevski
Dates work performed:	1 - 23 June 2021 - closing meetings 1-2 July 2021
Draft report issued:	3 September 2021

Final report issued:





LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)

LSBU	Design		Poor system of internal control.
	Effectiveness		Non-compliance with key procedures and controls places the system objectives at risk.
SBC	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.
SBA	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.

LSBU GROUP SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High		
Medium		
Low		

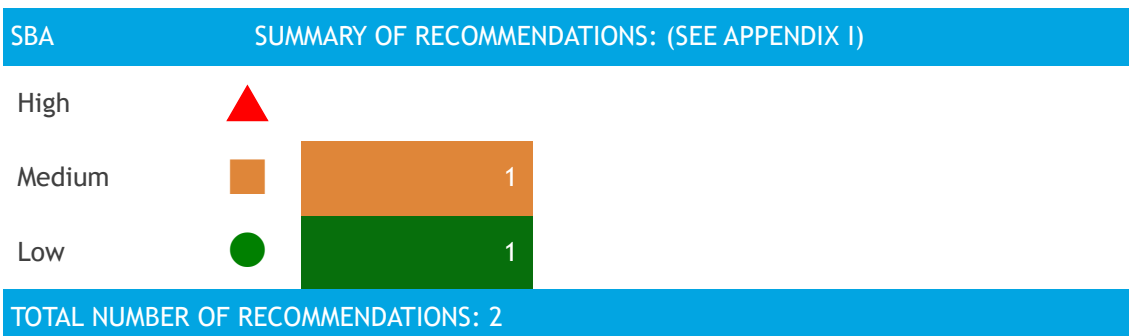
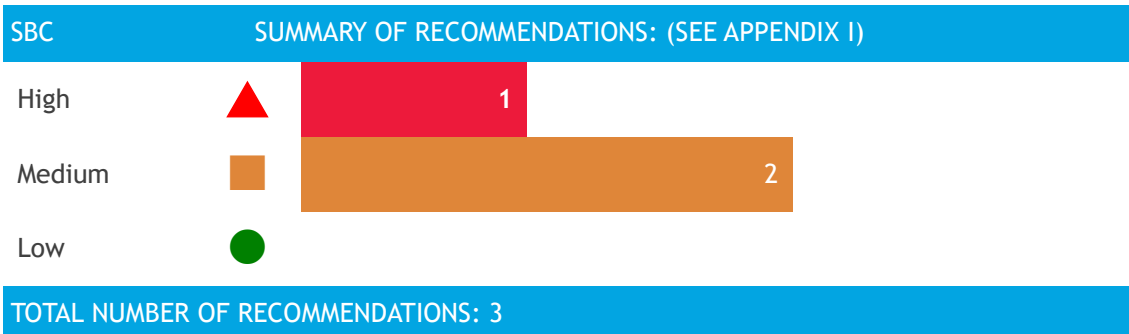
TOTAL NUMBER OF RECOMMENDATIONS: 1

LSBU SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I)

High		
Medium		
Low		

TOTAL NUMBER OF RECOMMENDATIONS: 3

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY



BACKGROUND:

In accordance with Group's 2020/21 Internal Audit Plan, BDO has undertaken an audit of IT Disaster Recovery (IT DR) across the LSBU Group. The audit covered London South Bank University (LSBU), South Bank Colleges (SBC) and South Bank Academies (SBA).

The purpose of the audit was to provide assurance over the design and operational effectiveness of IT DR policies and procedures in place across the Group.

IT DR involves a set of policies, tools and procedures to enable the recovery or continuation of technology infrastructure and systems following a natural or human-induced disaster. Effective IT DR planning is essential to ensuring that an organisation is able to respond to system failures in the event of a major incident or disaster, in order to maintain operations of all critical systems.

Separate Active Directory (AD) instances and networks are implemented in all audit entities. Currently, there is a decentralised approach to the delivery of IT services including recovery arrangements.

The information security audit undertaken in 2020 identified that although there is little inter-connectivity at the IT level between the entities, they had a similar cyber security risk profile. Similar or identical findings have been identified across all the entities during this review.

All entities have a traditional on premises IT environment that is more demanding from the perspective of IT DR than a cloud computing model. The Group intends to develop a more integrated, standardised and agile operating environment which could also simplify the future DR efforts and plans.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

LSBU

In December 2020, the University suffered a major cyber security incident that resulted in a complete loss of networking services. The Cyber Security insurance policy was activated and a third party IT company engaged by the insurance company and, with the cooperation of LSBU's IT team, took the lead in the recovery process. The first IT services were recovered six weeks after the incident. The University is still in the process of recovery.

As part of the new design of the IT environment, an updated overall backup solution is planned but this is still in the design and pre-implementation phase. It is expected that the new solution will be implemented in the second half of 2021. Prior to the start of this audit, a new Group Director of IT & Digital Transformation took up post.

SBC

The College's Head of IT is responsible for day to day IT operations as well as for planning and coordinating IT DR activities. The College's business operations were also impacted by the cyber security incident suffered at the University, as the Finance and HR system is shared between institutions. DR responsibilities for these two systems sit with the University.

SBA

IT services and IT DR operations for the academies are outsourced to Pallant Management Services Ltd. SBA was not impacted by the cyber security incident.

SCOPE AND APPROACH:

The review considered:

- Identification, recording and monitoring of organisational IT DR risks
- Roles and responsibilities for IT DR and data backups, including an assessment of key person dependencies and commitment from senior management
- IT DR policies, plans and procedures
- IT DR testing and training
- System and data back-ups.

Our approach was to conduct interviews to establish the controls in operation for each of our areas of audit work. We sought documentary evidence that these controls were designed as described. We evaluated these controls to identify whether they adequately address the risks.

Specifically we:

- Reviewed the organisational structure for IT DR, including the identification and monitoring of risks, and assessed its adequacy and alignment with the size and structure of the University, College and academies.
- Assessed whether roles and responsibilities have been appropriately defined and identified key person dependencies. Through interviews with staff with IT DR responsibilities we assessed whether these responsibilities are understood.
- Reviewed the IT DR process documentation, policies, procedures and framework to assess whether these were aligned with best practice, were complete and up-to-date. We also established whether appropriate metrics are defined and what scenarios would trigger the necessary response mechanisms.
- Verified when the IT DR plans were last reviewed and communicated to staff (and any third parties) and roles and responsibilities were clearly understood. We also assessed whether plans are accessible in the event of an incident and assessed how confidential information contained within the plans is protected.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

- Reviewed the IT DR training arrangements in place to assess frequency and content of training and whether it aligned to staff roles and responsibilities.
- Reviewed the IT DR testing arrangements including the frequency of testing, monitoring of tests, and recording of results and the implementation of corrective actions / recommendations. We determined whether the IT DR testing covers all critical IT systems and how management gains assurance that systems can be recovered within the required parameters.
- Reviewed how a lessons learned process enhances disaster recovery practice, especially in a light of the recent major security incident.
- Reviewed the arrangements for backing up systems and data to assess whether these are sufficient to enable the organisation to recover its infrastructure, data and services within acceptable parameters. This included consideration of the storage and location of backups.

GOOD PRACTICE:

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

LSBU

- Only secure IT systems are rolled out in live production as part of the current recovery process
- A formal lessons learned exercise is scheduled after the full recovery of IT services.

SBC

- The College has implemented redundancy on several ICT infrastructure levels such as internet connectivity, firewall configuration, Active Directory¹ and email infrastructure.

SBA

- A third party IT provider delivers a cloud backup solution for both academies.

KEY FINDINGS:

We have documented nine findings; four of high significance, four of medium significance and one of low significance. The ratings of the findings are based on the size and risk profile of the entity, but also on the best practice implemented within comparable organisations.

The nature of the findings are similar across all entities and as a result the recommendations are also similar. Therefore, a joint approach to the remediation of the issues, co-ordinated by the Group, should be considered.

The distribution of findings by entity is as follows. We have also included one Group-level finding.

¹ Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

Group

The Information Security audit report (August 2020) identified the need for a Group approach to information security. This report also highlights a need for a group approach to, and governance over, IT disaster recovery.

We have raised an overarching high significance finding relating to the lack of a Group-level IT DR structure and policy that will enforce governance and management over IT DR operations at all levels.

LSBU

We have raised three findings relating to the University; two of high significance and one of medium significance.

The high significance findings relate to the lack of a formal Risk Assessment (RA) and Business Impact Analysis (BIA) to identify the key DR metrics, and the lack of a formal IT DR plan that outlines the roles and responsibilities, approach, testing and training activities.

The medium finding relates to the current backup practice not being in line with good practice.

SBC

For SBC we also raised three findings; one of high significance and two of medium significance.

The high significance finding relates to the lack of a DR site and a formal IT DR plan that outlines the DR metrics, roles and responsibilities, approach, testing and training activities.

The two medium findings relate to the identification of IT DR metrics and weaknesses in backup practices.

SBA

For the academies we raised two findings, one of a medium significance and one of a low significance.

The medium finding relates to the lack of formal IT DR Plan and requirements.

CONCLUSION:

LSBU

At the time of the cyber security incident, which resulted in the complete loss of network services, LSBU did not have an IT DR plan in place and this is still the case. There had also been no regular testing of IT recovery capabilities. These issues contributed to the recovery process exceeding expected usual recovery timeframes for similar organisations.

Given the seriousness of the incident and based on the weaknesses identified in other areas, we can provide no assurance on the design, and limited assurance on the effectiveness, of the current IT DR practice at LSBU.

SBC

Whilst basic backup controls are in place and there is resilience in the design of some aspects of IT infrastructure, a number of weaknesses have been identified in DR practices at SBC. Therefore, we are able to provide limited assurance over the design and the operational effectiveness of the IT DR controls in place.

SBA

Whilst basic backup controls are in place, we identified a number of improvement opportunities, again related to the main IT DR practices. As a result we are able to provide a

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY


moderate assurance over the design and limited assurance over the operational effectiveness of the IT DR controls in place.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

DETAILED FINDINGS - GROUP

RISK:

- RISKS RELATED TO IT DR NOT IDENTIFIED, DOCUMENTED AND ADDRESSED
- ROLES AND RESPONSIBILITIES WITH REGARDS TO IT DR AND DATA BACKUP ARE NOT APPROPRIATELY DEFINED, ASSIGNED AND UNDERSTOOD OR CREATE AN INCREASED DEPENDENCY ON KEY INDIVIDUALS
- IT DR DOCUMENTATION IS INSUFFICIENT, OUTDATED OR INACCESSIBLE IN THE EVENT OF AN INCIDENT
- FAILURE TO RESPOND TO AN ADVERSE EVENT AND RECOVER AS EXPECTED DUE TO A LACK OF TRAINING AND /OR TESTING - KEY FINDINGS

Ref	Sig.	Finding
1		<p>We were unable to identify the existence of an appropriate governance structure to oversee IT DR activities at Group level and across the entities.</p> <p>In particular, we noted that there are no formal business processes for the following:</p> <ul style="list-style-type: none"> - Planning of IT DR activities, including methodology for risk assessment and business impact analysis - IT DR training - Reporting and performance monitoring of IT DR activities - Regular review and update of the IT DR controls and framework <p>Achieving an effective and consistent approach to IT DR throughout the organisation requires a system with structures and processes in place to guide decision-making, accountability, control and behaviour.</p> <p>An inadequate IT DR governance structure and policy could lead to the absence of a clear IT DR mandate. A clear DR policy is essential for driving DR initiatives throughout the Group and the entities. Without a clear mandate, DR operations could be severely impacted and cause significant impact to ongoing operations as happened in the recent incident.</p> <p>Without predefined methodology for RA and BIA, there is risk of inconsistent identification of basic DR metrics across the Group entities.</p>

RECOMMENDATION:

The LSBU Group should:

- Assign a governance body with authority to steer the overall IT DR direction across the Group. This body should hold the responsibilities for approval of:
 - Overall IT DR strategy
 - IT DR related policies
 - Organisation of IT DR
 - Introduction of improvements to the IT DR on all levels within the Group.
- Develop, communicate and enforce a formal IT DR policy. The policy should establish the:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

- Objectives for IT DR across the Group
- Roles and responsibilities for IT DR both Group and entity levels
- Process for regular DR training for relevant staff, after every change in the DR framework and/or DR staff
- Processes for monitoring and reporting performance over IT DR matters
- Requirements for regular testing and lessons learned.
- Formally document the methodology and the scope for IT DR, Risk Assessment and Business Impact Analysis.
- Enforce that lessons learned from the major cyber security incident are communicated to all entities within the Group and incorporated in the new IT DR practices.

MANAGEMENT RESPONSE:


Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

DETAILED FINDINGS - LSBU

RISK: RISKS RELATED TO IT DR NOT IDENTIFIED, DOCUMENTED AND ADDRESSED - KEY FINDINGS

Ref	Sig.	Finding
2		<p>LSBU has no documented IT DR risk assessment nor business impact analysis. Furthermore, existing IT DR documents are dated between 2004 and 2006 and do not hold relevant information to the current IT environment.</p> <p>Consequently, the relevant and updated primary metrics for disaster recovery, the Recovery Time Objective (RTO), Recovery Point Objective (RPO) and the Maximum Tolerable Period of Disruption (MTPD) for the key critical process have not been identified nor documented to reflect the current IT environment.</p> <p>Creating an effective DR plan starts with the documenting of a risk assessment and business impact analysis. A risk assessment is a document that contains a description of potential risks to the functioning of an organisation. A business impact analysis predicts the consequences of disruption for a business function and process and gathers information needed to develop recovery strategies. The analysis should identify how quickly and to what moment in time the essential business units and/or processes have to return to full operation following a disaster situation.</p> <p>The lack of these processes increases the risk that the University may not recover in a timely and structured manner following a major incident, as seen with the recent incident.</p>

RECOMMENDATION:

LSBU should document and perform an IT DR risk assessment. Following the completed recovery of the IT environment, based on a formal Group methodology for IT DR, LSBU should identify and document the following:

- The most crucial business functions and systems
- The staff and technology resources needed for operations to run optimally
- The timeframe within which the functions need to be recovered for LSBU to restore operations as close as possible to a normal working state.

Furthermore LSBU should:

- Ensure that the Business Impact Analysis development process has senior management dedication, support, sponsorship and an extensive involvement of IT and end users
- Formally define the key metrics to the DR environment, the RPO, RTO, and the MTPD for the processes of interest.

MANAGEMENT RESPONSE:

Responsible
Officer:


LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

RISKS:

- ROLES AND RESPONSIBILITIES WITH REGARDS TO IT DR AND DATA BACKUP ARE NOT APPROPRIATELY DEFINED, ASSIGNED AND UNDERSTOOD OR CREATE AN INCREASED DEPENDENCY ON KEY INDIVIDUALS
- IT DR DOCUMENTATION IS INSUFFICIENT, OUTDATED OR INACCESSIBLE IN THE EVENT OF AN INCIDENT
- FAILURE TO RESPOND TO AN ADVERSE EVENT AND RECOVER AS EXPECTED DUE TO A LACK OF TRAINING AND /OR TESTING

Ref	Sig.	Finding
3		<p>The University does not have a formal IT DR plan that defines the operational roles and responsibilities to be taken in the event of an incident. At present the University only has a formal high-level document outlining the overall incident response at the strategic level.</p> <p>Furthermore, we noted that there is no history of testing of the LSBU DR capabilities nor DR training for key staff.</p> <p>IT DR involves a set of documents, tools and procedures that enable the recovery and continuation of vital technology infrastructure and systems, following a natural or human-induced disaster. The central piece in this set is the IT DR Plan which defines the roles and responsibilities related to the recovery process, and testing of the organisational capabilities.</p> <p>The lack of a formally documented DR Plan and testing increases the risk that the IT services and IT business systems or data are not restored on time following a major disruption.</p> <p>Failure to provide the LSBU staff with adequate and up to date DR training increases the risk of personnel being unable to perform their related duties and responsibilities as required.</p>

RECOMMENDATION:

After the completed recovery of the IT environment, based on the Business Impact Analysis outcomes and in alignment with the Group IT DR policy, LSBU should develop a formal LSBU DR Plan. The plan should include:

- Detailed procedures to be followed before, during and after an IT disaster.
- A complete inventory of hardware and applications in order of priority. Each application and piece of hardware should have the vendor technical support information and contract number.
- Formal business-approved tolerance for downtime and data loss (DR metrics).
- Clear definition of key roles, responsibilities and parties involved during a DR event. Among these responsibilities must be the decision to declare a disaster and who has the authority to invoke the DR Plan.
- Communication plan with effective and reliable methods for communicating with employees, vendors, suppliers and customers.
- Statement that can be published on the LSBU website and social media platforms in the event of an emergency.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

- Alternative site with supporting documentation, if the primary office is not available.
- Operational procedures to ensure the protection of sensitive information during the event.
- Details on how DR will be tested, including the method and frequency of tests.

LSBU's management or the Group body responsible for IT DR should formally review and approve the new LSBU DR Plan.

In addition, LSBU should implement IT DR training for the new IT DR Plan for the staff involved in the DR operations.


MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

RISK: DATA MAY NOT BE ABLE TO BE RESTORED UPON SYSTEM FAILURE DUE TO WEAKNESSES IN THE BACKUP DESIGN OR OPERATIONAL PROCEDURES

Ref	Sig.	Finding
4		<p>The backup solution currently in place does not follow the 3-2-1 backup best practice rule, and there is only one copy of data backup stored on premise.</p> <p>In addition, we noted that the verification that the backup has been successful is based on reports produced by the backup software but not from formal backup test restoration testing.</p> <p>The current backup practices increase the risk that LSBU will be unable to recover the data, or recover in time, if access to the backups is required.</p>

RECOMMENDATION:

Based on a Risk Assessment and Business Impact Analysis, LSBU should consider further improvements to the current backup solution in addition to having a second off-site copy of the data backup.

After the completed recovery of the IT environment, LSBU should:

- Develop backup and restore plans according to the result of the Business Impact Analysis. These plans should be formally approved by management (or the Group body responsible for IT DR).
- Formalise the backup retention periods in correlation with retention periods defined by legal or business requirements.
- Develop additional operational backup and recovery management procedures including:
 - Job monitoring
 - Success/failure logging and reporting
 - Problem analysis and resolution
 - Backup storage management
 - Scheduling
 - Performance analysis
 - Capacity trending and planning
 - Policy review and analysis
 - Data backup and recovery testing and verification.
- Test a representative sample from the backups (e.g. system images, database, files) on a regular basis (e.g. at least annually). The results from the testing should be documented, any issues investigated and presented to a relevant governance committee for review.

MANAGEMENT RESPONSE:

Responsible
Officer:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY


Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

DETAILED FINDINGS - SBC

RISKS:

- ROLES AND RESPONSIBILITIES WITH REGARDS TO IT DR AND DATA BACKUP ARE NOT APPROPRIATELY DEFINED, ASSIGNED AND UNDERSTOOD OR CREATE AN INCREASED DEPENDENCY ON KEY INDIVIDUALS
- IT DR DOCUMENTATION IS INSUFFICIENT, OUTDATED OR INACCESSIBLE IN THE EVENT OF AN INCIDENT
- FAILURE TO RESPOND TO AN ADVERSE EVENT AND RECOVER AS EXPECTED DUE TO A LACK OF TRAINING AND / OR TESTING - KEY FINDINGS

Ref	Sig.	Finding
5		<p>We reviewed the DR function at SBC and noted the following:</p> <ul style="list-style-type: none"> - There is no off-site DR recovery location in a case of full site-wide IT incident - The IT Services DR Plan has not been formally approved - The IT Services DR Plan does not contain the operational roles and responsibilities relating to the DR function - There is no history of previous testing nor formal testing schedule - There is no formal training for responsible DR staff <p>The lack of a formally approved DR Plan increases the risk that the IT services and IT business systems or data are not restored on time following a major disruption.</p> <p>The absence of testing or infrequent testing could result in DR recovery environments that do not perform as required during a disaster.</p> <p>Failure to provide the SBC staff with adequate and up to date DR training increases the risk of personnel being unable to perform their related duties and responsibilities.</p>

RECOMMENDATION:

Based on the RA results and the criticality of the business processes (see also finding 6), SBC should identify a DR site, if the primary office is not available. This could also be managed at a Group level.

SBC should update its IT Services DR Plan with:

- A clear definition of key roles, responsibilities and parties involved during a DR event. Among these responsibilities should be the decision to declare a disaster and who has the authority to invoke the DR Plan.
- Identified DR metrics for the critical business functions and systems.
- Details on how the plan will be tested, including the method and frequency of tests.

SBC's management and the Group body responsible for IT DR should formally review and approve the plan.

Based on the updated IT Services DR plan, SBC should provide DR training for the staff involved in the DR operations.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY


MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

RISK: RISKS RELATED TO IT DR NOT IDENTIFIED, DOCUMENTED AND ADDRESSED - KEY FINDING

Ref	Sig.	Finding
6		<p>The identification of critical IT services and related DR metrics are not based on a risk assessment and did not follow a business approved methodology for identification of the criticality to the IT services.</p> <p>The absence of risk-based and business verified DR processes and procedures increases the risk that the IT systems are not restored on time.</p>

RECOMMENDATION:

Based on the recommended Group methodologies for Risk Assessment and Business Impact Analysis, SBC should document:

- The DR Risk Assessment and the most crucial business functions and systems
- The staff and technology resources required for operations to run optimally
- The period within which the functions need to be recovered for SBC to restore operations as close as possible to a normal working state
- The main metrics for IT DR, the Recovery Time Objective (RTO), Recovery Point Objective (RPO), and the Maximum Tolerable Period of Disruption (MTPD) for the key critical processes.

This exercise could also be managed at a Group level.


MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

RISK: DATA MAY NOT BE ABLE TO BE RESTORED UPON SYSTEM FAILURE DUE TO WEAKNESSES IN THE BACKUP DESIGN OR OPERATIONAL PROCEDURES

Ref	Sig.	Finding
7		<p>There is draft Backup policy that defines the backup strategy and current approach to the backup operations.</p> <p>However, we noted that the backup strategy has not been formally approved and there is there is ad-hoc restore testing of the backups.</p> <p>There is a risk that SBC will be unable to recover the correct data or recover in time if access to the backups is required.</p>

RECOMMENDATION:

Based on the risk assessment results and the criticality of the business process, SBC should update the backup strategy and the Backup policy and formally sign off the policy.

SBC should test representative samples from the backups and document the results from the exercise. The frequency of the backup tests should be also be communicated and agreed with the business.

MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

DETAILED FINDINGS - SBA

RISKS:

- ROLES AND RESPONSIBILITIES WITH REGARDS TO IT DR AND DATA BACKUP ARE NOT APPROPRIATELY DEFINED, ASSIGNED AND UNDERSTOOD OR CREATE AN INCREASED DEPENDENCY ON KEY INDIVIDUALS
- IT DR DOCUMENTATION IS INSUFFICIENT, OUTDATED OR INACCESSIBLE IN THE EVENT OF AN INCIDENT
- FAILURE TO RESPOND TO AN ADVERSE EVENT AND RECOVER AS EXPECTED DUE TO A LACK OF TRAINING AND / OR TESTING

Ref	Sig.	Finding
8	■	<p>SBA has a draft DR plan, with the objective to define general procedures for a contingency plan at the Academies.</p> <p>We reviewed the plan and the IT DR practice and noted that:</p> <ul style="list-style-type: none"> - The criticality of the business processes and the supporting IT systems have not been formally documented and included in the plan - The plan is a draft version and has not been approved - There is no history of IT DR testing - There is no formal training for responsible DR staff. <p>The lack of identification of critical business IT systems increases the risk that systems and data are not restored on time following a major disruption.</p> <p>The absence of testing or infrequent testing could result in DR environments that do not perform as required during a disaster.</p> <p>Failure to provide the SBC staff with DR training increases the risk of personnel being unable to perform their related duties and responsibilities as required during a disaster.</p>

RECOMMENDATION:

SBA should update its IT DR Plan with:

- The most crucial business functions and systems identified with consideration of the Group methodology for Business Impact Analysis.
- The timeframe within which the functions need to be recovered for SBA to restore operations as close as possible to a normal working state
- The main metrics for IT DR, the Recovery Time Objective (RTO), Recovery Point Objective (RPO), and the Maximum Tolerable Period of Disruption (MTPD) for the key critical processes.

SBA's management and group body responsible for IT DR should formally review and approve the plan.

SBA should test the updated IT DR plan at least an annual basis.

Based on the updated IT DR Plan, SBA should provide DR training to relevant staff.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY


MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

RISK: DATA MAY NOT BE ABLE TO BE RESTORED UPON SYSTEM FAILURE DUE TO WEAKNESSES IN THE BACKUP DESIGN OR OPERATIONAL PROCEDURES

Ref	Sig.	Finding
9		<p>At SBA all data is stored centrally on the school's IT servers which are backed up with predefined schedules and retention periods.</p> <p>The current backup strategy is documented in a draft Backup Policy and has not been formally agreed by management.</p> <p>In addition, we noted that a regular backup testing is not performed. We were informed that by the end of the year, weekly tasks for backup test restores would be added to the new IT Service Management System.</p> <p>There is a risk that SBA will be unable to recover the data or recover in time if access to the backups is required.</p>

RECOMMENDATION:

Based on the criticality of the business processes assessed by SBA management, the backup strategy should also be agreed with SBA management. Any changes should be reflected in the Backup policy which should also be finalised.

SBA should regularly test representative samples from the backups and document the results from the restores any deviations analysed.

MANAGEMENT RESPONSE:

Responsible
Officer:

Implementation
Date:

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY





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.




Stuart Johnston	Group Director of IT & Digital Transformation (LSBU)
Malvina Gooding	Group Director of IT Services (LSBU)
Graeme Wolfe	Head of Information Security (LSBU)
Adam Bird	IT Services Manager & ProMonitor Support (SBC)
Moshe Franco	Head of ICT Infrastructure (LSBU)
Suresh Seyani	Infrastructure Systems Engineer (LSBU)
Dan Cundy	Executive Principal (SBA)
Ewaen Igbiovvia	Service Manager (Pallant Managed Services)

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

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, IT DISASTER RECOVERY

APPENDIX II - TERMS OF REFERENCE

PURPOSE OF REVIEW:

The purpose of the audit is to provide assurance over the design and operational effectiveness of IT DR policies and procedures in place 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:

- Inability or failure to recover business critical IT systems in a timely manner due to:
 - Risks related to IT DR not identified, documented and addressed
 - Roles and responsibilities with regards to IT DR and data backup are not appropriately defined, assigned and understood or create an increased dependency on key individuals
 - IT DR documentation is insufficient, outdated or inaccessible in the event of an incident
 - Failure to respond to an adverse event and recover as expected due to a lack of training and /or testing
 - Data may not be able to be restored upon system failure due to weaknesses in the backup design or operational procedures.

SCOPE OF REVIEW:

For the university, College and Academies the review will consider

- Identification, recording and monitoring of organisational IT DR risks.
- Roles and responsibilities for IT DR and data backups, including an assessment of key person dependencies and commitment from senior management.
- IT DR policies, plans and procedures.
- IT DR testing and training.
- System and data back-ups.

However, 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 three control environments, and that we will be providing assurance over controls in these environments. If this is not the case, our estimate of audit days may not be accurate.

LONDON SOUTH BANK UNIVERSITY GROUP, IT DISASTER RECOVERY

APPROACH:

- 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.
- Specifically we will:
- Review the organisational structure for IT DR, including the identification and monitoring of risks and assess its adequacy and alignment with the size and structure of the University, College and Academies.
- Assess whether roles and responsibilities have been appropriately defined and identify any key person dependencies. Through interviews with staff with IT DR responsibilities, we will assess whether these responsibilities are understood.
- Review the IT DR process documentation, policies, procedures and framework to assess whether these are aligned with best practice, complete and up to date. We will also establish whether appropriate metrics are defined and what scenarios would trigger the necessary response mechanisms.
- Verify when the IT DR plans were last reviewed and communicated to staff (and any third parties) with IT DR roles and responsibilities. We will assess whether plans are accessible in the event of an incident and assess how confidential information contained within the plans is protected.
- Review the IT DR training arrangements in place to assess frequency and content of training and whether aligned to staff roles and responsibilities.
- Review the IT DR testing arrangements including the frequency of testing, monitoring of tests, and recording of results and the implementation of corrective actions / recommendations. We will determine whether the IT DR testing covers all critical IT systems and how management gain assurance that systems can be recovered within the requested by the business/management parameters.
- Review how the lessons learned process enhance the DR practices, especially in a light of the recent major security incident.
- Review the arrangements for backing up systems and data to assess whether sufficient to enable organisation to recover its infrastructure, data and services within acceptable parameters. This will include consideration of the storage and location of backups.

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 ©2021 BDO LLP. All rights reserved.

www.bdo.co.uk

Agenda Item 5

CONFIDENTIAL - RESTRICTED TO MEETING PARTICIPANTS	
Paper title:	Fact Finding & Lessons Learned, LSBU IT Audits & Cloud Migration
Board/Committee:	Group Audit & Risk Committee
Date of meeting:	28 October 2021
Author(s):	Nicole Louis – Chief Customer Officer
Sponsor(s):	Dave Phoenix – Group CEO
Purpose:	For discussion & approval
Recommendation:	The committee is required to note the findings of the fact-finding exercise and support the recommendations for changes to project and programme oversight

Executive Summary

This paper sits alongside the IT Review undertaken by the Group Director of IT following the ransomware attack in 2020. The IT review focuses on questions around infrastructure, capability and capacity of the IT function. This paper seeks to consider issues of IT governance and oversight. To assess this area it undertakes a deep dive into changes around the cloud based services and considers the effectiveness of triangulation through use of internal audit and other means.

Fact Finding

Internal Audits and Assurance

Audits Conducted

Between June 2013 and October 2021, LSBU commissioned five individual internal audits relating to various aspects of IT. Three audits were conducted by PWC and two by BDO. In addition, PWC conducted a follow-up phishing report in 2014 and in 2018, the IT department commissioned a professional assessment from a third party considering specific aspects of IT and particularly, readiness for cloud data migration. The approach to audit and especially the phishing tests would be considered to follow good practice.

The audits show that IT governance and security were areas which represent a high degree of risk to the organisation throughout the period of the audits. However, each audit had a specific focus and covered different aspects of IT, with some looking at general governance and controls including physical (estate) security, others looking specifically at data (cyber) security and / or phishing, one providing a general 'state of the nations' in relation to the IT risk landscape and the most recent audit looking at IT disaster recovery.

Time Period	Type	Auditor	Classification
June 2013	IT Controls & Phs'g	PWC	High Risk
May 2014	Phishing Report	PWC	N/A
Sept 16	Data Security	PWC	High Risk
Oct 17	IT Risk Diagnostic	PWC	High Risk
Aug 20	Information Security	BDO	Limited assurance
(Sept 21	IT Disaster Recovery	BDO	No assurance)

Themes and Assurance

In the main, each audit identified a specific catalogue of risks requiring management responses and these are summarised in each report. The exceptions to this are the 2017 IT Risk Diagnostic report which was the most wide-ranging audit undertaken, and the 2014 phishing report which was a follow up test.

The 2013 audit focussed on IT controls and phishing with a number of management actions set out. Broadly, the identified areas of risk did not re-occur in the subsequent audits with the exception of password security and complexity (a recurring theme) and physical security linked to restricted access to IT server and network areas. This would seem to indicate that areas identified were being addressed.

The 2014 was a specific phishing stress test with recommendations focussed on user education. This tends to be a challenge across HEIs due to the volume of students and the increased use of mobile devices.

The 2017 IT Risk Diagnostic Audit highlighted a significant number of risk areas, most of which were newly identified in that they were not set out in the previous two audits which in contrast, were narrow in scope. The report was a comprehensive assessment focussing on the maturity of controls within IT set against the risk environment and the IT department produced an action

plan (dated January 2018) which went to the University Executive. The plan covered 23 individual actions with some already marked as completed, and others due to complete no later than December 2018.

The next audit was undertaken nearly three years later in August 2020 and this focussed specifically on information security. This was the first audit covering the entire group with three sub-set reports. These findings highlighted a number of new areas of risk for LSBU in contrast to the 2016 and 2017 reports, although there were some recurring risk areas that should have been completed by December 2018. Recurring risk areas were:

1. Governance and resourcing for IT security (single person accountability, lack of resource)
2. Password complexity
3. USB encryption
4. Passwords (policy and approach)

In addition, significant areas of risk were identified for the first time including the configuration of the IT network, back-up policy, anti-virus configuration, legacy server and desktop operating systems (i.e. Window 7) and local administrator accounts. Whilst the configuration of the network was a new risk in this report, the 2017 audit picked out 'the high volume of legacy hardware which may result in major outages or business disruption'. The management response at the time set out that 'hardware replacement is under review and a priority on our technical roadmap'. It is not clear what hardware was replaced between the audit findings in 2018 and the cyber incident in December 2020 however by 2020, the university was still operating with a significant amount of legacy hardware at the server and end-user level.

The actions were in the process of implementation before the attack with for example pilots undertaken on changes to password protocols. The actions arising from this audit are still being completed and are overseen by the IT Security and Resilience Board. Across all three institutions, a number of management actions have been completed, a number have been started and are partially complete, whilst one or two yet to be tackled. Progress is being continually tracked.

The final audit undertaken in September 2021 post the attack focussed on disaster recovery and found a lack of systems, policies and procedures in this area. This was also identified as a gap in the 2017 audit with the management response setting out a completion date of December 2018. The recent audit indicates that this was not addressed as documentation sourced on previous DR processes was dated 2006.

Observations.

The use of audit appears to follow good practice with use of phishing tests being a strength and actions being closed. Indeed in 2017 a specific audit looking at risk was undertaken to inform future development of the IT environment. There are limited recurring themes but a regular high risk flag on IT and a number of actions were taking a prolonged period to close. The underlying state of the IT environment and the focus on response to individual actions rather than addressing systemic issues would perhaps question the:

- i) strength of IT leadership in terms of potentially knowledge, understanding, capability.
- ii) and or a culture preventing the overall scale of the challenges being reported.

The former point seems to align with the report form the Group IT Director.

Fact Finding and Lessons Learned

LSBU Strategy to Migrate Data and Services Form IBM Cloud to Public Cloud

As background LSBU had migrated a large proportion of activity to the cloud working with IBM between 2013-2014. This involved material being housed on servers provided by the supplier. In this case servers were housed at LSBU and a duplicate centre in Amsterdam. Not all services (e.g., student data) were expected to migrate.

Timeline of Related Activities

MARCH
2018

1. A Data Hosting Investment Strategy was proposed by David Mead (then Executive Director of ARR) and was approved by the University Executive on 28th **March 2018**. This paper set out the strategic approach proposed to migrate data and services from the IBM private cloud to a public cloud. The paper was high-level and set out the broad strategy for data hosting, indicative cost savings over a period of time and the risks of a 'do-nothing' scenario. The Executive supported the proposal.
2. At the time of developing the data hosting investment strategy, IT was a business unit operating within the PSG called ARR and the data migration project was conceived and internally owned by the then Director of IT Tony Crewdson. It was supported by David Mead and the then Chief Operating Officer Ian Mehrstens. This is relevant because later-on, all individuals directly associated with project ownership left the organisation.
3. Key drivers to initiate the project at that particular time were the existing leasing arrangement with IBM was coming to an end in February 2019 and unless alternative arrangements were secured, there would be a mandatory contract continuation of five years. The IBM solution was expensive, and the two data centres (UK and Amsterdam) were poorly configured meaning that there was not a 'fail-safe' in place in the event that one data centre failed. In addition to this, the hardware in the data centres was being managed and maintained directly by the IT Operations teams at a significant management overhead.
4. The Data Hosting Investment Strategy paper did not contain detailed timelines for implementation but referenced that it could take between 2 to 3 years to complete giving an indicative timeline of between March 2018 (conception) and March 2021 (maximum endpoint). The strategy set out stages as follows: -
 - 20% of the data and services currently hosted on the IBM private cloud migrated to a public cloud solution with a target date of February 2019
 - The remaining 80% of services currently hosted on the IBM private cloud transferred to the new LSBU data centre to be 'right sized' before transitioning off premise. (It was not anticipated that all applications would be suitable to transfer to public cloud, i.e. it was possible that some would be decommissioned and other transferred to SAAS)
 - Migration to the public cloud for the services not initially transferred would likely take between 18 months and 2 years.
5. The investment paper did not set out detailed costs of implementing the three-year programme but described financial savings of moving from the IBM cloud to the public cloud solution over a forward looking 5-year period.

APRIL
2018

6. Around the same time that the Executive was asked to approve the strategy, as a parallel piece of work, Alex Denley (then Deputy Director of IT Innovation and Transformation) was asked to undertake a cloud readiness assessment to determine if LSBU was fit and ready to migrate to public cloud. This was a mechanism to stress test the strategy set out by Tony Crewdson and the assessment used external supplier A.N.S. and took three months to complete. The assessment report provided in **June 2018** to Tony Crewdson and David Mead concluded that the university was not ready to move to public cloud with the two main findings being:
- LSBU operated with publicly routable IP addresses (meaning it would need to completely re-architect the LSBU network before proceeding)
 - That the LSBU server estate had significant technical debt and needed significant 'housekeeping' and a number of technical issues to be resolved to make migration to the cloud effective and efficient

It is unclear if this report and the impact of the findings on the pace of the migration strategy were shared with the Executive Director but they were not shared with the wider LSBU Executive.

SEPT
2018

7. In September 2018 Shan Wareing, took over responsibility for ARR and IT from Ian Mehrtens

NOV
2018

8. In **November** 2018 - the LSBU Executive and the LSBU Board received a Corporate Strategy Progress Report which read: "The Data Centre migration to a hybrid cloud solution is now in progress, with the new architecture commissioned, and transfer will be completed by January 2019."

FEB
2019

9. On 20th February 2019, an update was brought to the LSBU Executive providing an update on the data hosting strategy. The paper provided an update on progress of the initial stage of data centre migration; the shift from services hosted on the IBM Private Cloud to the Dell on premise cloud (VX Rail), and the decommissioning of end-of-life HP on-premises servers with the migration of associated software to the Dell on premise cloud. The update said:

- "The migration saw LSBU leave the IBM cloud solution as the 5-year contract came to an end and move to a hybrid model of a Dell supplied datacentre and the public cloud. This has reduced the operational cost of data centre storage by 50% per annum (approximately £500K per annum). It further went on to say:
- **Data Centre Migration Phase One:** Migrating from IBM cloud to Dell local cloud to reduce the operational cost of hosting data. Completed in January 2019.
- **Data Centre Migration Phase Two:** Migrating from on premise HP servers to Dell local cloud to improve the reliability and performance of servers. Due to complete in June 2020

APR
2019

10. In April 2019, Tony Crewdson and David Mead left LSBU. There were no risk flags with respect to onsite data storage nor any indications that the process being followed was anything other than 'routine'
11. In April 2019, Alison Chojna was appointed Acting Executive Director of ARR (replacing David Mead). Due to the swift departure of both David and Tony, Alison was unable to

receive a handover. There was no project or resource plan specific to the project and no separate project manager. There was also no dedicated IT department roadmap to set out specific priorities for completion that year and the migration to cloud was not set as a priority project for Alison Chojna to pick up.

NOV
2019

12. Nicole Louis assumes executive responsibility for IT in November 2019 as Shan Waring left to take up a new role. In November 2019 Alison Chojna submitted a capital funding request for £380k as 'Phase 3' of the cloud migration project which was approved. The deliverables for this stage of the project would be an updated technical assessment to allow the team to start baselining the transition of services to the public cloud including timeframe and costs.

NOV
2019

13. A project initiation document (PID) was prepared for Phase 3 of the migration work (dated 19th November 2019) and the intention was for this work to run as a project within the IT department, overseen by Alex Denley, Director of IT Innovation and Transformation. The scope of work was scheduled to run from February 2020 and October 2020. A significant point to note is that this stage of the project now included the requirements of Lambeth College which were not part of the original project scope.

14. Despite undertaking the scoping work, the Covid pandemic and the resulting shift to all staff working fully remotely halted the start of service migration as the IT team felt that this was too much of a risk to undertake the work during the time where staff were fully dependent on service continuity and the outlook for lockdown remained unclear. The cyber incident and recovery work diverted all IT staff from any project work not directly associated with incident recovery.

JUN 20

15. In June 2020 an update was given to FPR on the progress of the Physical and Digital Resources Sub-Strategy of the LSBU Corporate Plan by the ICT and Estates and Academic Environment Departments. The report was brought to the Executive ahead of FPR for noting. The relevant section about migrating to cloud technologies read:

"2.5.1. There are many benefits to cloud computing and the hybrid-cloud model being developed for the Group takes advantage of the benefits of public cloud, such as scalability, mobility, cost savings, flexibility and disaster recovery, whilst maintaining control of critical operations. Valuable data can still be secured centrally and locating critical services closer to users will minimise latency and optimise speeds.

- *The LSBU Group will operate within a hybrid cloud model.*
- *The majority of services will operate in public cloud, beginning with a single cloud tenancy and maturing to a multi-cloud tenancy.*
- *The remaining on-premise services will be delivered through our hyper-converged solution.*
- *We will capitalise on the multi-site nature of the LSBU Group by building disaster recovery capabilities between locations.*
- *One infrastructure that will service the LSBU Group, reducing complexity and providing a consistent user experience.*

2.5.2 In Dec 2018, LSBU migrated away from the IBM private cloud onto a new, hyper-converged on-premise data centre. This was phase one of moving to public cloud. The SBC infrastructure is also currently on-premise and is now at end of life. The Group

Microsoft Azure public cloud tenancy is currently being built, with the first services expected to migrate to public cloud in 2020.

2.5.3 As space becomes available in the LSBU data centre, the cluster will be divided, with half moving to SBC, to accommodate the remaining on-premise services. This will build resilience back into the on-premise solution.

Lessons Learned

21. All of the stages required to achieve full migration to the public cloud and associated risks were not clearly set out to the Executive at the beginning, specifically that this was a programme rather than an 'internal IT project' and that the stages of work would require significant re-structuring of the IT network as well as work to address legacy servers. The time and resources required to re-architect and simplify, as well as delivering a capability model to upskill the workforce for cloud readiness were not part of the initial strategy paper and the 'remedial or preparatory work' would have competed for resources alongside all other work delivered by the IT department. Whilst the LSBU Executive approved the migration strategy, this was not therefore followed up by a fully scoped out programme plan covering resources, milestones, timelines, key deliverables etc. with central oversight
21. At the local level it appears that there was no programme or project manager assigned to what was undoubtedly going to be a complex scope of work extending over a sustained period of time. Without professional project management, there was little by way of project documentation to support the transfer of knowledge and expectations when personnel changed.
22. The related work for the initial stage was overseen within the line of management of IT and ARR, with periodic narrative updates provided to the Executive and FPRC. However there did not seem to be a formal, detailed, evidence-based review of project progress beyond the high-level statements provided to the Executive and FPRC which are limited in detail and fail to identify risks. There was no clear escalation of risks through internal oversight process such as the risk register nor at the time issues raised through performance review meetings leading to a lack of organisational knowledge about the work being undertaken.
23. The changes in IT, ARR and COO leadership resulted in a loss of institutional knowledge around priorities and expectations for this work. At the point that the IT Director and Executive Director of ARR left the university, there was no IT department operating roadmap in place, just a high level ARR roadmap. There were also new and emerging priorities for the department which shifted the focus of leaders.

Recommendations for Change

24. All projects or programmes should have desired outputs clearly defined from end-to-end at the point of scoping and have supporting milestones and noted inter-dependencies. All projects or programmes fitting criteria of scale or risk/complexity and impact should be overseen by the Group Executive or an alternative delegated authority and provide regular, standardised reporting including RAG and risk ratings. Large scale

projects such as large capital projects or complex cross institutional; projects such as LEAP appear well captured but there may be risk around high impact projects focused within single services if these are not clearly escalated. A cross institutional review of 'project work' will be undertaken and oversight arrangements confirmed if required.

25. The scale of risk associated with this program would have been expected to be escalated through the risk register process. A review of the operational effectiveness of this system will be undertaken with, I required, training of Directors and Deans.
26. There is a question around the effectiveness of our CAPEX planning process which has been already been identified for review. The focus on new large capital has limited focus on a multi-year understanding of the infrastructure replacement costs.

End