ISC16D009

Title:	***Risks in Information Services 2016-17***
Author:	Jonathan Colam-French
Date:	9 September 2016
Circulation:	ISSC – 18 October 2016
Agenda:	ISC16A001
Version:	Final
Status:	Open

Issue

This paper is to draw the committee's attention to the risks that have been identified associated with the services provided by Information Services.

Recommendation

Members of ISSC are asked to receive the report. The risk register is used to help inform planning and development of the ISD programme of work.

Resource Implications

None

Risk Implications

There are no extra risks associated with this report.

Equality and Diversity

There is no impact on groups with protected characteristics.

Timing of decisions

Report is for information.

Further Information

Enquiries about the content of this paper should be directed to Jonathan Colam-French, Director of Information Services, on ext 3858, email: j.colam@uea.ac.uk

Background

The risk register lists those high level risks applying to ISD services. Risks relating to services are categorised by the likelihood and potential impact. The overall severity of the risk is summarised as per the matrix below:

Likelihood				
	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Negligible	Low	Medium
		Low	Medium	High
		Impact		

ISD Risk Register 2016/17

Risks are categorised as relating to staff (loss of knowledge, support, availability), building (fire, flood, bomb, sit-in, contamination), resources (power, data, software, hardware, IT systems, PCs, finances), or security/compliance (legislation, confidentiality, integrity and availability of data).

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
1	Staff	Current staffing models do not adequately provide cover for current or emerging University operational requirements driven by changes to technology, emerging threats or increased demand	During 2015/16 the restructuring of IT support allowed us to focus existing staff resource to better meet priority areas, including front line support and to a limited extent Learning Technology. Agreement has been reached for four additional developers in the CIS Group which will help to address the backlog of work in this area. Looking forward - adherence to enhanced IT security compliance has further limited the resource available, especially within the infrastructure teams. An external review of staff structures has taking place in order to identify resource gaps and associated risks and recommendations will be built into the Digital Strategy that is under development.	M	H	H
2	Staff	Current staffing models are insufficient to support emerging requirements driven by opening hours and increased student numbers	The restructuring of IT Support over the summer 2015 allowed us to provide increased first line IT support at weekends. Library front of house teams remain lean and unfortunately we had one unplanned closure of the building and several occasions where we came very close to closing.	M	M	M
3	Staff	Limited staff resource to support new initiatives	Across all areas of ISD we have a robust prioritisation process to ensure that resources are deployed to support the most valuable developments and initiatives. Four additional	M	L	L

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
			developers have been released into the CIS Group to work on the backlog of requests. As a result of the IT Restructuring in 2015 the size of the Learning Technology Teams have increased significantly. A review of all of the IT Support Team has been undertaken and recommendations will be built into the Digital Strategy.			
4	Staff	Medium to long-term sickness of key staff	Ensure knowledge transfer between team members, in general good progress has been made on this. Ensure documentation is up to date. Secondment from another team or specialist 'buy in'.	L	M	L
5	Building	Loss of a Data Centre including fire, flood, loss power or cooling. A review by Estates undertaken in August 2015 identified previously unknown single points of failure on the mechanical and electrical infrastructure, until these are resolved the likelihood of failure has increased from Low to Medium.	Ensure that Estates DR and BC planning includes adequate provision for the Data Centres. Ensure service specific DR and BC plans are adequate, with service split across data centres. Work with Estates to ensure the resolution of Data Centre single points of failure are included within planned maintenance programmes. Fire and leak detection systems installed. Monitoring and alerting configured for all mechanical and electrical systems. UPS and generators installed in both data centres.	M	H	H

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
6	Building	Denial of access to building due to evacuation, contamination, student activity, power loss, fire, flooding, etc.	Ensure service specific DR and BC plans are adequate Ensure remote access to key resources is achievable	L	M	L
7	Building	Loss of irreplaceable Library collections due to fire or flood	Leak detection system in Archives. Shut off valves installed. DR plan reviewed annually to ensure prompt action in event of fire or flood.	L	M	L
8	Building	Library collections space is inadequate for the projected growth.	New Collection Development policy Short term – 3-5 year plan for withdrawals plus refurbishment of space on floor 02 to provide additional compact storage (unfunded). Medium term - business case for extension as otherwise no further scope for accommodating project growth in collections beyond 2020.	M	M	M
9	Building	Library study space & related infrastructure inadequate for actual and projected numbers of students over next 5 years	Short term: refurbishment of large IT open access suite (unfunded) Refurbishment and repurposing of space on reading floors (unfunded) would provide up to an additional 150 study spaces, still 100 short of the estimated 250 needed to maintain student/study space ratios. Refurbishment of old PG reading room and expansion into room currently being used as the temporary prayer facility to create Social Learning Café (unfunded) Additional toilet facilities to meet minimum standards for the numbers in the building (unfunded) Replacement of toilet stack and related drainage (unfunded) Plans for rolling stack on Floor 02 (unfunded).	H	H	C

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
			In turn this could provide up to an additional 150 study spaces. Business case for extension as otherwise no further scope for the additional 100 spaces (over & above the 150) needed to maintain student/study space ratios in light of University expansion.			
10	Resources	New initiatives do not meet expectations	Ensure requirements are clearly articulated as part of the business case. Oversee delivery with robust project management.	L	M	L
11	Resources	Failure to manage the growth and proliferation of business information systems	The process for requesting new business systems has been reviewed, updated and reviewed by the CIS Board. A request workflow and proforma template request form has been implemented.	M	H	H
12	Resources	Service failure / downtime	Ensure suitable process for upgrading minimises downtime. Adhere to ISD change control process Monitor and manage the service Document and monitor dependencies Run regular patching Update software to latest supported version and run regular patching Ensure annual maintenance plan is in place Ensure that users of services are aware of the need for their DR plans to cover for the loss of services. Provide out of hours support for agreed key services.	M	H	H
13	Resources	Data feed failure leading to a proliferation of data errors across systems	Ensure strict change controls in line with ISD processes	L	M	L
14	Resources	Systems (component) failure	Ensure key hardware is resilient and failover system available	M	L	L

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
15	Resources	Financial or technical failure of major remote service / content provider resulting in loss of services	Ensure service or provider specific DR and BC plans are adequate Ensure alternative means to provide service equivalent or content are identified, albeit this is not always possible.	L	H	M
16	Resources	Financial failure of major provider of Library stock	Ensure alternative supply chains are in place, we have also changed the way that payment is managed making it more staggered.	L	M	L
17	Resources	External supplier changes contract, product or support provision	Improve the management of key supplier relationships. Ensure that rigorous procurement processes are in place. Monitor the market to inform strategic planning.	L	M	L
18	Resources	Reading list project fails to secure academic buy-in	Plan for academic buy-in using self-service facilities on Talis. Explore whether policy needs extension to full mandate to ensure academic take-up. Improve communications and link up with Learning Technology for communications and Blackboard embedding.	H	M	H
19	Security/ compliance	New or emerging threat to IT infrastructure	Investment is being made via the IT Security Project, but further investment may be required as this is a rapidly evolving field. Ensure the security of the infrastructure, underpinned by an appropriate awareness campaign. Ensure that hardware and Operating Systems that are no longer supported are removed from network or segregated.	H	H	C

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
20	Security/ compliance	Allocation of invalid access to buildings or resources	Validation on data feeds where possible. Audited process for assigning user rights.	L	M	L
21	Security/ compliance	Data corruption	Ensure strict change control Backup data Ensure client anti-virus software is up to date Remove elevated users' rights (root/Admin access) when these are not required Raise user awareness to phishing and malware Ensure that users of services are aware of the need for their DR plans to cover for the potential corruption of data.	L	H	M
22	Security/ compliance	Data retained beyond its required life span	Develop and audit data retention policies. Encourage staff to apply retention policies to email folders and consider introducing a policy of active retention / passive deletion for email. Ensure that owners of business information systems are aware of the need to implement data retention policies.	H	L	M
23	Security/ compliance	Hosting of copyrighted / libellous / inappropriate / illegal / malicious materials	Rapid Takedown policy; Staff training; Conditions of Computer Use. In addition, the Digital Innovation Team now provide guidance on compliance issues for web material. Strong web governance	M	M	M
24	Security/ compliance	Loss of equipment or inappropriate decommissioning leading to security vulnerability or data loss	Ensure decommission process is adhered to and is audited Ensure contracts for leased equipment include adequate data wiping	M	M	M
25	Security/ compliance	Non-compliance with legislative or regulatory regimes	Staff training Compliance managed through central team Records management processes	M	M	M

Number	Category	Risk	Mitigation	Likelihood	Impact	Overall
			Privacy impact assessments integrated into the development of all new and changed systems and processes Audits			
26	Security/ compliance	Unauthorised access to a system or data	IT security project is overseeing the implementation of additional monitoring tools. Ensure compliance with CoCU and ISD policies Education of users regarding appropriate use Run frequent security audits Security monitoring	H	H	C
27	Security/ compliance	Loss or unauthorised distribution of data	Data only made available to approved users. Mandatory staff training on data protection imposed on all staff handling personal data Ensure Data Processing Agreements are in place for all data processed by other users and organisations on our behalf. Enhanced advice and guidance on data sharing best practice. Implement data loss prevention tools in Microsoft products	H	H	C