University of East Anglia

ISC14D013

Title:	***Risks in Information Services 2014-15***
Author:	Jonathan Colam-French
Date:	27 January 2014
Circulation:	ISSC meeting 6 February 2014
Agenda:	ISC14A002
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 2014/15

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).

Category	Risk	Mitigation	Likelihood	Impact	Overall risk assessment
Staff	Current staffing models do not adequately provide cover for current or emerging University operational requirements driven by changes to technology or emerging threats	Seek additional funding for posts associated with ensuring IT security or restructure and reduce service in other areas to address this key risk.	H	H	C
Staff	Current staffing models are insufficient to support emerging requirements driven by opening hours or increased student numbers	Keep University hours of opening under review and consider changes to staffing model as appropriate. Ensure that implications on staffing of new ventures and courses is raised in a timely fashion Further development of self-service options.	H	M	H
Staff	Limited staff resource to support new initiatives	Monitor requirements and look for additional income. Manage expectations and ensure that robust prioritisation is in place	H	L	M
Staff	Medium to long-term sickness of key staff	Ensure knowledge transfer between team members Ensure documentation is up to date Secondment from another team or specialist 'buy in'	L	M	L
Building	Loss of a Data Centre including fire, flood, loss power or cooling	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. Fire and leak detection systems installed. Monitoring and alerting configured for all mechanical and electrical systems. UPS and generators installed in both data centres.	L	H	M
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
Building	Loss of irreplaceable Library collections due to fire or flood.	Leak detection system in Archives. Shut off valves installed.	M	M	M

Category	Risk	Mitigation	Likelihood	Impact	Overall risk assessment
		DR plan reviewed annually to ensure prompt action in event of fire or flood.			
Resources	New initiatives do not meet expectations	Ensure requirements are clearly articulated as part of the business case. Oversee delivery with robust project management.	M	M	M
Resources	Failure to contain and/ or manage the growth and proliferation of business information systems	Ensure that all departments are required to provide a business case to underpin new systems requests to be overseen by the CIS Board.	M	M	M
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
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
Resources	Systems (component) failure	Ensure key hardware is resilient and failover system available	M	L	L
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	L	H	M
Resources	Financial failure of major provider of Library stock	Ensure alternative supply chains are in place	L	M	L
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

Category	Risk	Mitigation	Likelihood	Impact	Overall risk assessment
Security/ compliance	New or emerging threat to IT infrastructure	Ensure that appropriate investment is made to ensure the security of the infrastructure, underpinned by an appropriate awareness campaign.	H	H	C
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
Security/ compliance	Data corruption	Ensure strict change control Backup data Ensure client anti-virus software is up to date 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
Security/ compliance	Data retained beyond its required life span	Develop and audit data retention policies. Ensure that owners of business information systems are aware of the need to implement data retention policies.	M	L	L
Security/ compliance	Hosting of copyrighted / libellous / inappropriate / illegal / malicious materials	Rapid Takedown policy; Staff training; Conditions of Computer Use	M	M	M
Security/ compliance	Loss of equipment or inappropriate decommissioning leading to security vulnerability or data loss	Ensure decommission process is adhered to and is audited	L	M	L
Security/ compliance	Non-compliance with FOI/EIR	Staff training Compliance managed through central team Records management processes	L	M	L
Security/ compliance	Unauthorised access to a system or data	Ensure compliance with CoCU and ISD policies Education of users regarding appropriate use Run frequent security audits	L	H	M
Security/ compliance	Loss or unauthorised distribution of data	Data only made available to approved users. Staff training Ensure Data Processing Agreements are in place for all data transferred to other users and organisations.	H	H	C