University of East Anglia

ISC13D024

Title:	***Risks in Information Services 2013-14***
Author:	Jonathan Colam-French
Date:	23 January 2014
Circulation:	*Members of ISSC*
Agenda:	ISSC meeting 6 February 2014
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 consider the report.

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 which have been identified from an analysis of low level risks recorded in individual service area risk logs.

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 2013/14

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), or security/compliance (legislation, confidentiality, integrity and availability of data)

Category	Risk	Mitigation	Likelihood	Impact	Overall risk assessment
Building	Loss of a Data Centre	Ensure this is covered by Estates DR/BC plan Ensure Service specific DR and BC plans are adequate	M	H	H
Building	Denial of access to building	Ensure Service specific DR and BC plans are adequate Ensure remote access to key resources is achievable	L	M	L
Building	Fire	Ensure this is covered by Estates DR/BC plan Ensure Service specific DR and BC plans are adequate	L	H	M
Building	Flood	Leak detection systems installed Ensure this is covered by Estates DR/BC plan Ensure DR and BC plans are adequate	L	H	M
Building	Student activity	Ensure Service specific DR and BC plans are adequate Ensure remote access to key resources is achievable	L	M	L
Resources	Client software failure	Run regular patching Update software to latest supported version	M	L	L
Resources	Data feed failure	Ensure strict change controls in line with ISD processes Monitor and review the feed and log files	L	M	L
Resources	External supplier changes contract, product or support provision	Improve/Manage relationship with supplier	L	M	L
Resources	Failure of specialist hardware	Ensure annual maintenance plan in place	L	M	L
Resources	Failure to manage changes to a service leading to software failure	Ensure strict change controls in line with ISD processes	M	L	L
Resources	Lack of resilient service	Ensure Service specific DR and BC plans are adequate	L	M	L
Resources	Power loss	Ensure this is covered by Estates DR/BC plan	L	H	M
Resources	Service degradation or loss of performance	Actively monitor services using SCOM Provide Out Of Hours Support	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	M	H	H

Category	Risk	Mitigation	Likelihood	Impact	Overall risk assessment
		Document Dependencies and Monitor			
Resources	Systems (component) failure	Ensure hardware is resilient and failover system available	M	L	L
Resources	Unavailability of external (non UEA) system	Improve/Manage relationship with supplier	L	H	M
Security/ compliance	Allocation of invalid access to buildings or resources	Validation on data feeds where possible Audited process for assigning user rights.	L	L	N
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	L	L	N
Security/ compliance	Data retained beyond its required life span	Develop and audit data retention policies	M	L	L
Security/ compliance	Hosting of copyrighted / libellous / inappropriate / illegal / malicious materials	Rapid Takedown policy; Staff training; Terms 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 too and is audited	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	Unauthorised distribution of data	Data only made available to approved users Ensure Data Protection Agreements are in place for all data transferred to other users and organisations.	M	M	M
Staff	Lack of staff resource	Monitor requirements and look for additional income	M	M	M
Staff	Lack of timely support from supplier	Improve/Manage relationship with supplier	L	M	L
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’	M	M	M
Staff	Staff crises	Ensure knowledge transfer between team members Ensure documentation is up to date Secondment from another team or specialist ‘buy in’	L	M	L