GISP1. Risk assessment and risk management

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	University information services and computing and telecommunication systems will be subject to regular risk assessment and management.
Objective	• To ensure that the security of the University's information services and computing and telecommunication systems is reviewed on a regular basis. • To determine risks, their impact and the managed response required to remove the risk or reduce its impact.
Policy	1.1. The security risks associated with all University information services will be reviewed at least annually and a risk log produced.
Responsibility	Service owners are responsible for ensuring that risk assessment and management is undertaken
Incident management	New risks identified should have their impact promptly assessed and a managed response determined.
Audit and accountability	Annually updated risk logs for all information services within UEA will be reviewed by the IT Forum (ITF) and IT Support Managers before being submitted to the Information Strategy and Services Committee (ISSC). ITCS will co-ordinate this activity.
Implementation	• ITCS will produce a Risk Log Template for use with centrally managed services and by Faculties. • ITCS will identify a list of all services they operate and using the Risk Log Template will record any significant security risks threatening these services and mitigating action to be taken. • Faculties will identify a list of all services they operate and using the Risk Log Template will record any significant security risks threatening these services and mitigating action to be taken.

	• Those responsible for a service should review the Risk Log for that service at least annually and whenever there is a significant change to the service, or whenever a serious security incident affects the service. • Risk Logs for all services will be reviewed annually by ITCS with the IT Forum and IT Support Managers and thereafter submitted for consideration by ISSC. This activity to be co-ordinated by ITCS.