Security Risk Log – SCVA Tickets Server

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [1]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access to server	Housed in secure and controlled environment with access control on entrance.	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Replace faulty equipment	ITCS	H	H	DLR= 12/8/09	Within6 months
Record Deleted	Restoration from backups - 8 Week tape rotation – network backup	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Inappropriate access to paper records stored on system	User Domain passwords are applied, users only have rights to authorised Folders	ITCS	L	M	DLR= 12/2/08	Acceptable risk

[1] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – HUM Server

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [2]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access to server	Housed in secure and controlled environment with access control on entrance.	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/8/09	Acceptable risk
Record Deleted	Restoration from backups - 8 Week tape rotation – network backup	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Inappropriate access to paper records stored on system	User Domain passwords are applied, users only have rights to authorised Folders	ITCS	L	M	DLR= 12/2/08	Acceptable risk

[2] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – File Store / Shares

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [3]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ICTS	L	M	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access to server	Housed in secure and controlled environment with access control on entrance.	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Record Deleted	Restoration from backups - 8 Week tape rotation network backup	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Inappropriate access records stored on system	User Domain passwords are applied, users only have rights to authorised Folders within share.	ITCS	L	M	DLR= 12/2/08	Acceptable risk

[3] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – PC Security

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [4]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	H	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ITCS	L	H	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access	Housed in secure office with access control on entrance.	User	L	L	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Warranty of Next Business Day replacement of faulty parts for 3 Yrs	Hum IT	L	M	DLR= 12/2/08	Acceptable risk
File Corruption	Restoration from backups - 8 Week tape rotation – network backup	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Domain Logon	User Domain passwords are applied	ITCS	L	L	DLR= 12/2/08	Acceptable risk

[4] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Mac Security

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [5]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access	Housed in secure office with access control on entrance	Users	L	L	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Warranty of Next Business Day replacement of faulty parts for 3 Yrs	Hum IT	L	M	DLR= 12/2/08	3 months
File corruption or Deletion	Users have no access to shares, no auto backup, each users responsible for there own backups	Users	L	H	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Inappropriate access to files	User Password in use	ITCS	L	M	DLR= 12/2/08	Acceptable risk

[5] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – EAFA Server

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [6]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Network infrastructure						
Network Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Switch Failure	Replace faulty equipment	ITCS	L	M	DLR= 12/2/08	Acceptable risk
Physical security						
Unauthorised physical access to server	Housed in secure and controlled environment with access control on entrance.	EAFA	M	L	DLR= 12/2/08	Acceptable risk
Storage and data security						
Hardware Failure	Replace faulty equipment	HUM IT Support	L	M	DLR= 12/8/09	Acceptable risk
Record Deleted	Restoration from backups - 8 Week tape rotation – network backup	ITCS	L	L	DLR= 12/2/08	Acceptable risk
Authentication and authorisation						
Inappropriate access to paper records stored on system	User Domain passwords are applied, users only have rights to authorised Folders	ITCS	L	M	DLR= 12/2/08	Acceptable risk

[6] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Budget

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [7]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Inflation not taken into account.	Budget is still at a good level 2-3K short of where it needs to be, but this has been offset by previous Extra funds awarded.	IT Manager	H	L	DLR= 28/10/10	Acceptable risk
Increased Hardware cost not taken into account	See above	IT Manager	H	L	DLR= 28/10/10	Acceptable risk
Academic research grants (1K per person)	No effect on the Budget, but generally effect staff resource at end of financial year.	IT Manager	M	M	DLR= 28/10/10	Acceptable risk
Extra Fund awards	If any awarded then further staff resource taken	IT Manager	L	M	DLR= 28/10/10	Acceptable risk
New academic staff	Increase Numbers puts more pressure on budget offset by previous Extra funds awarded.	IT Manager	M	L	DLR= 28/10/10	Acceptable risk

[7] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Communications

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [8]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Internal						
Faculty to IT Team, No or little notice of room moves or new staff starting	Increase workload that may delay other work.	Faculty	L	M	DLR= 28/10/10	Acceptable risk
Faculty ill informed of changes from IT Team	Unexpected scenarios may cause delays in work.	IT Manager	L	M	DLR= 28/10/10	Acceptable risk
New course design not communicated to IT Team	May put pressure on resources both financial and time	Faculty	L	M	DLR= 28/10/10	Acceptable risk
External						
ITCS to Faculty, no notice to updates and changes to central systems	Unexpected changes could cause delays	ITCS	M	M	DLR= 28/10/10	Acceptable risk
IT team to External suppliers late deliveries	Concertinaed workload may cause delays in job completion.	IT Manager	M	M	DLR= 28/10/10	Acceptable risk

[8] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work – External To Faculty (UEA)

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [9]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Windows 7 upgrade						
Need to respond to new critical developments at short notice	It will have an impact on the work load of the Technicians.	Faculty Manager	M	M	DLR= 29/10/10	Acceptable risk
Managed print service						
Inability to secure User's engagement in project.	User training will be vital, changes in the way some people work may be necessary.	Faculty Manager	M	M	DLR= 29/10/10	Acceptable risk
May not give users the time scales or the functionality required	Central priorities may be different from the faculty priorities as in SITS not giving the functionality required or the delays in network printing that have occurred since central took over the project from HUM.	Faculty Manager	M	M	DLR= 1/11/10	Acceptable risk

[9] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Plan

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [10]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
IT Budget will be scraped due to financial constants.	5 year plan could be redeveloped into 6 years thus decreasing budget by 15%, Machines would decrease work rate.	Faculty Manager	L	M	1/11/10	Acceptable risk
Member of IT staff leave	All planed work would have some delay as 1 person represents 50% of the workforce	Faculty Manager	M	M	1/11/10	Acceptable risk
The program of work is overly ambitious	Poor planning may lead to unacceptable delays in the project and standard work	Faculty Manager	L	M	2/11/10	

[10] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Quality

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [11]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
PC replacement on a 5 year cycle	Ensures fast reliable machines to ensure minimum loss of time to staff	Faculty Manager	M	M	DLR= 2/11/10	Acceptable risk
Ensure where possible that systems incorporate the Staff desktop	Keeps Virus scans, security up to date, use central shares for backups.	Faculty Manager	L	H	DLR= 2/11/10	Acceptable risk

[11] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Reputation

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [12]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
National and international Events i.e. Lit Fest	Agreed support from central to provide factices for events	Faculty Manager	L	H	DLR= 1/11/10	Acceptable risk
External to HUM	Network failures, virus infestation, security breach, Web falure	ITCS	L	H	DLR= 2/11/10	Acceptable risk

[12] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Resource

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [13]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
PC Support Tecs	Illness, Holidays, agreed reciprocal arrangement with central to provide cover	Faculty Manager	H	L	DLR= 2/11/10	Acceptable risk
Technician leaves	Loss of Knowledge about HUM systems	Faculty Manager	M	M	DLR= 2/11/10	Acceptable risk
Loss of IT budget due to financial constraints	Life cycles extended, slower machines meaning users take more time	Faculty Manager	L	H	DLR= 28/10/10	Acceptable risk

[13] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column

Security Risk Log – Faculty programme of work - Scope

Risk	**Mitigation**	**Owner**	**Likelihood** High/ Medium/ Low	**Impact** High/ Medium/ Low	**Date identified/ reviewed** *DRI=dd/mm/yy / DLR=dd/mm/yy*	**Timescale for action** Within 3 months/ Within 6 months/ Within 1 yr/ Acceptable risk [14]
Description of the risk	*Mitigating action already taken or planned to be taken*	*Central service division or Faculty responsible for monitoring and mitigating the risk*	*Likelihood of occurrence*	*Impact of risk on service security*	*Date risk identified(DRI) or date last reviewed (DLR)*	*Estimated timescale for mitigating action to be taken*
Failure's external to facility leads to delays	Planed expenditure increases, users become disenfranchised i.e. Network printing	ITCS	M	M	DLR= 29/11/10	Acceptable risk

[14] Where denoted as 'Acceptable risk' justification should be given in the Mitigation column