

	Compliance risks).	
Disaster recovery and planning	<ul style="list-style-type: none"> • Computer system failures or loss of data. • Destruction of property, equipment, records through fire, flood or similar damage. 	<ul style="list-style-type: none"> • IS recovery plan. • Data back up procedures and precautions. • Insurance cover. • Disaster recovery plan for alternative accommodation.
Procedural and systems documentation	<ul style="list-style-type: none"> • Lack of awareness of procedures and policies. • Actions taken without proper authority. 	<ul style="list-style-type: none"> • Proper documentation of policies and procedures. • Audit and review of systems.
Information Technology	<ul style="list-style-type: none"> • Loss/corruption of data eg donor base. • Lack of technical support. 	<ul style="list-style-type: none"> • Appraisal of system needs and options. • Security and authorisation procedures. • Implementation and development procedures. • Use of service and support contracts. / Outsourcing • Disaster recovery procedures. • Insurable loss.