Job			Recommendation	Risk Category	Criticality	Target Date	Recommendation
C	8	SI - Moving Forward	0 Paper records to be secured	S	S	30-Jul	All records stored on paper that contain personal, confidential or sensitive information must be secured in lockable filing cabinets and the key removed when not in use. Key control must be formalised so that only authorised officers can access records.
C	8		0 Office door to be locked and key control	S	S	30-Jul	The door to the office (that contains the PC and all records) should be locked when not in use - particularly at night. Key control must be formalised so that only authorised officers have keys.
C	8	SI - Moving Forward	0 Memory Stick Use	S	S	30-Jul	TOO LARGECurrently there are 4 USB flash drives used by the project team. Encryption software (TrueCrypt) is available for use but there is n business requirement for sensitive information to be stored or transporte on them. All sensitive information should be stored in an appropriate drive on a server which is backed up regularly. USB flash drives should only be used for non-sensitive information. It is against the GSI/GCSx policy to store protectively marked data (or data that should
C	8		0 Signing Out System for Memory Sticks	S	M	30-Jul	USB flash drives should be signed out and back in by staff when taken out of the office.
C	8	SI - Moving Forward	0 Retrieve Missing Memory Stick	S	S	30-Jul	Only 3 of the USB flash drives were stored in the office. The fourth is believed to be with another member of staff. Until the drive is recovered we do not know the exact nature of the data held and cannot be sure that unencrypted, sensitive information is not stored on it. This flash drive must be located and retrieved immediately and handed over to Internal Audit for further investigation.
C	8		0 Relevant Staff to have GCSx Training	S	S	30-Jul	Anyone in the project team who has access to sensitive information and may be required to share this with other departments or organisations

must go through GSI/GCSx training.

o
d

l,