Scope of Service: -

Globallink is going to provide a SaaS based application to Fidelity. The FX Connect and GTSS application will be utilised for trade matching as once trades get executed they are sent to the matching platform, the broker also sends their trades into the platform. Once matched settlement details are auto applied to the trade and sent to the custodian for settlement.

Fidelity **confidential** information which includes FX and time deposit details, fund static data, such as name, LEI custodian, to facilitate matching and settlement in Large no. of Records (50,000+).

ESR Inherent Risk- High

•Financial Impact: The data being shared with the Globallink includes Fidelity Confidential data. There is a risk that spear phishing could be targeted at the supplier through which the Fidelity fund data, and employees’ data could be compromised. This could lead to financial and regulatory repercussions for Fidelity.

•Reputational Repercussions: In case of any data breach through misconfigured security settings on their operating environment could lead an individual to exploit and have access to Fidelity funds data which in turn could have regulatory and reputational repercussions for Fidelity.

TrustPortal has confirmed that they cannot decrypt the Fidelity data and business has also confirmed the same that supplier cannot decrypt the data and access the keys. Hence the control is marked as not applicable.

Data stored in the TrustPortal SaaS is pushed by FIL Robots. We cannot see this data as its encrypted with keys specific to the client. However we can setup specific data retention processes for the archival and deletion of specific data

Clarification Objective:

Immediately on termination of the FIL TrustPortal Contract, all FIL systems and data will be deleted

As the data cannot be decrypted without TrustPortal being in place, then there is no data retention post-contract. Any data that FIL wish to retain would be obtained from FIL robots

The requirements of the backups is done in conjunction with Fidelity, including AWS data centre selection for primary, secondary and DR and their frequency

Please see contract for details of backup agreements (see 1.2)

Clarification Update:

All data stored in TrustPortal is PPK encrypted at rest - hence by definition it is encrypted when backed up

In addition standard AWS backup is encrypted

Please see previous questions regarding encryption employed by TrustPortal