SUBSERVICE ORGANIZATION CONTROL CONSIDERATIONS

In all processing environments, there are certain controls and procedures that the subservice organizations should be responsible for performing to help ensure the quality of service and integrity of the processing. The controls in place at RISLA represent only a portion of the overall internal controls of the subservice organizations, and RISLA has designed its controls under the assumption that certain controls are implemented by the subservice organizations. The implementation of certain controls at the subservice organizations is necessary to enhance the efficacy of the controls and to achieve certain control objectives.

This Section describes certain controls that should be in place to achieve the control objectives identified in Section 4. The Complementary Subservice Organization Controls presented below should not be regarded as a comprehensive list of all controls that the subservice organization should employ.

UAS Control Considerations

1. The subservice organization should perform nightly backups of all transaction data.
2. The subservice organization should replicate data backups off-site.
3. The subservice organization should maintain and test a disaster recovery plan and a business continuity plan.
4. The subservice organization should maintain a redundant infrastructure and conduct failover testing on a regular basis to help ensure uptime of systems.
5. The subservice organization should monitor and patch all servers and computers.
6. The subservice organization should deploy AV protection on all servers and computers.
7. The subservice organization should maintain relevant systems in a secure server room equipped with climate control and fire suppression systems.
8. The subservice organization should maintain logical access controls that help ensure the access is authorized appropriately.
9. The subservice organization should have a change management process to help ensure hardware and software updates are authorized and tested, and that users are notified of scheduled outages and deployment of changes.
10. The subservice organization should maintain all relevant systems in a physical secure environment.
11. The subservice organization should complete user change requests are completed as instructed.
12. The subservice organization should conduct monthly credit reporting and distribution of monthly borrower statements.
13. The subservice organization should process the pending payments daily that are entered by RISLA.
14. The subservice organization should make RISLA aware of any processing errors identified.

Microsoft Azure Control Considerations

1. The subservice organization should restrict access to system resources to properly authorized individuals to the infrastructure.
2. The subservice organization should authorize, test and approve changes prior to implementation of new infrastructure; and changes to existing infrastructure.
3. The subservice organization should record, classify and track to resolution incidents and problems to the infrastructure.
4. The subservice organization should limit physical access to the data centers to properly authorized individuals and to monitor and maintain environmental controls to protect computer equipment within the data centers