# GLIB Internal Controls – SLOTH

## SLOTH System Specifications

1. Vendor Products
   1. Azure
      1. Web Application
      2. Database
   2. CyberSource
      1. Credit Card Payment Processor
   3. Stackify
      1. Logging Platform
   4. Sparkpost
      1. Email Provider
2. System will not contain PII
   1. Found PII will be removed
3. Transaction Types:
   1. Income
      1. From External Clients
   2. Recharge
      1. From Internal, University Clients
4. SLOTH User Authentication
   1. Web Interface: CAS via Office 365
   2. REST Interface: System assigned randomly generated tokens per user
5. SLOTH User Authorization
   1. Managed on application database
   2. Application Admin:
      1. Creates/removes/edits user access by request via ServiceNow
      2. Held by SLOTH Applications Admin and IT Applications Admins as necessary
      3. Role assignment approved by Business Manager
6. Transaction/Data Entry
   1. Recharge
      1. Automatic from customer activity via ANLAB Application
      2. Processed as a Feed
      3. Final approvals required by Business Manager
   2. Income
      1. Automatic from CyberSource reporting API
      2. Processed as a GL Feed
      3. Approval automatic
7. Audit and Logging
   1. All activity logged and stored to both to local database and external vendor, Stackify
   2. Audit Logs accessible by IT Applications Admins and Developers as necessary
8. System Change Requests
   1. Change Requests submitted to ServiceNow and/or GitHub Issue

## Scheduled Reviews/Reconciliations

1. Monthly:
   1. Business Analysts review batch successes and resolve any errors.
   2. Fiscal Officers perform ledger review
2. Annually:
   1. Application Admin and Business Manager review user and role assignments
   2. IT Management to review Azure system access
   3. IT Management to review Azure database access