In order to ensure growth and future competitiveness in the telecommunications service market, RODH Inc. needs to address a few issues in their accounts payable processes. Many of the discrepancies noted are deviations from typical industry standards, and should be addressed to keep RODH on par with their competitors and the industry as a whole. Outlined below are the most critical accounting and IT risks and possible courses of action for their resolution.

### Accounting Risks

- **AP clerk separation of duties is insufficient, exposing RODH to possible fraudulent accounting practices (high risk.)**
  - **Solutions**
    - Hire additional accounting clerk or repurpose a current clerk, reducing existing AP clerk’s areas of permission; divide transactional duties so that no one person is allowed to create and authorize transactions.
    - Adding an employee to the accounting department will distribute workload during reporting periods, reducing or eliminating the need for employees from other departments to complete accounting tasks (another high-risk area.)

- **The process for purchase order and invoice processing leaves RODH open to potential impropriety and inventory manipulation. This is yet another area where AP clerks have the majority of the responsibility over many interconnected recording processes and therefore have little oversight of their actions (moderate-high risk.)**
  - **Solutions**
    - Segregate duties of vendor creation/maintenance and purchase requisitions.
    - Lower $50,000 threshold for necessary staff accountant approval
    - Require mandatory approval of purchase requisitions over a given dollar amount to be converted to purchase orders

### IT Risks

- **Access control policies for employees are poorly implemented and maintained. Employees are given permission across departments, permissions are not revoked in a timely fashion and there seems to be a lack of access control policy (high risk.)**
  - **Solutions**
    - Implement and maintain a strict personnel access policy including:
      - Documented process for user permission modifications
      - Privileges restricted to job function
      - Job function changes should be followed within 3 days with access permission changes
      - Individuals other than IT staff should have physical access restrictions to mission-critical systems

- **The business continuity plan in place is glaringly inadequate, and could potentially be the highest risk area if not for the relatively low likelihood of a catastrophic data loss. Data retention and integrity should be of the highest concern to a firm, due to the increasing digital nature of business processes and record keeping (moderate-high risk.)**
  - **Solutions**
    - System-wide backups should occur weekly, and duplicates stored off-site
    - Transactional data should be backed up every day so that any short-term data loss can be re-created from transaction logs.
    - Integrity of backups should be tested quarterly and restoration process should be tested annually

Addressing these risks will position RODH to operate as efficiently as possible, while avoiding potential unnecessary costs and promote their growth to a FORTUNE 500 company and beyond.

---

**Team Members:** Brian Barlow, Chirag Chandna, Inna Hrudzetskaya, Abhay Kshirsagar, Kenneth Wunderle