Executive Summary

Technology Outsourcers of Georgia (TOOG) has just negotiated the acquisition of a financial services company, Financial Data Processing (FDP), to enhance its portfolio of enterprise management solutions; and, is in need of information assurance and risk management services through their systems consolidation and re-calibration transition.

The acquisition raises significant risks to TOOG in that FDP's financial transactions involve funds ownership and currency transfer information. In this domain, client information protection concerns are paramount, more so than TOOG's ever had to address before, along with the information sharing requirements set by regulatory agents.

This document seeks to provide guidance to reduce risk respective to these concerns and develop a flexible framework upon which TOOG can appropriate and audit FDP's systems. It identifies critical areas that TOOG's administrators must focus on as they gain control of systems, and provides guidance on strategies to re-engineer processes. An effective approach will need to address concerns relating to Organizational Security, Asset Classification and Control, Information Security Coordination, Physical and Environmental Control, Computer Network Management, System Access Control, Business Continuity Management, and Compliance[1].

[1] The advise contained herein is based on a review of Peltier's recommendations in "How to Complete a Risk Assessment in 5 Days or Less" (2009), and on the U.S. General Accounting Office's "Information Security Risk Assessment: Practices of Leading Organizations" (1998).

Risk Concerns and Transition Focus Areas

FDP handles sensitive funds transfer data that exposes TOOG to regulatory data sharing constraints and potential client liability claims. The transition to absorb FDP's systems requires TOOG to adopt a strict data access policy, while allowing the system engineers to gain sufficient knowledge to revise controls and transfer information assets. Whatever strategies are agreed upon will depend on continued fealty to follow the laws and regulations of the jurisdictions within which FDP and TOOG operate.

As system architecture and regulatory priorities are settled, TOOG's administrators will want to create a plan to work through the following risk management considerations[2]. These guidelines are intended to reduce the exposure to loss of data or breach of systems by disaffected employees or rogue elements during the early stages of the administrative transition[3]. They are expressed concisely herein, but in a manner that is hoped will facilitate a more detailed strategy.

1. Administrative Stakeholders and Command Policy

   The organizational and command structure of the new enterprise must be resolved at once. Authority over functional area ownership and decisions must be clearly expressed to the new organization. A transition plan should include details of how overlap in functions will be addressed, how facilities will distribute the work load, and establish intermediate gatekeepers to authorize any transactions that would impact the cash position of the enterprise.

[2] See GAO report for details on how to establish risk management practices in a financial services agency
[3] See Peltier's "Sample Threat Checklists" and "Gap Analysis Using A Combination Of Standards and Laws"

2. Organizational Processes, Systems and Controls Management

   The transition teams will require documentation on organizational workflows, their support systems and control policies. The priority should be to identify and corroborate authorized users for each system layer according to their role needs. Each functional area will have a designated owner or escalation partner.

   All system input and output ports should have traffic patterns analyzed to be sure port controls are up to date. The set of rules on the firewall should include constraints on MAC addresses and authorized applications. Benchmarking goals should be set based on daily, weekly and cyclical network bandwith demand.

3. Client Contractual Risks and Fund Transfer Policy

   Given the nature of financial risk exposure that arises in this acquisition, TOOG's administrators must ensure that the regulatory concerns that arose during discovery are addressed by the system administrators. Only authorized agents should establish fund transfer requests. A transitional gatekeeper authorization scheme should be established to ensure proper surveillance of use of funds. Cyclical FDP client service expectations and fund transfer schedules must continue to be met. Website, server and data hosting contractual obligations need to be well documented. Jurisdictional mercantile, tax and transport regulations must be cleared by the legal team, and system transition plans need to incorporate functional system requirements to continue to meet jurisdictional concerns.

Sources

Peltier, Thomas R. (2009). *How to Complete a Risk Assessment in 5 Days or Less*. Auerbach Publications. Last accessed April 6, 2010 at Books24x7, http://0-common.books24x7.com.catalog.kcls.org/book/id_30507/book.asp

United States. (1999). *Information security risk assessment Practices of leading organizations : a supplement to GAO's May 1998 executive guide on information security management*. Washington, D.C. (P.O. Box 37050, Washington, D.C. 20013): The Office.