



Breeding Ground for Risk (and Vendor Due Diligence)

The Breeding Ground

Outsourcing business processes has been common practice in today's banking world. From janitorial to information security services, banks are looking to vendors so that concentration and internal resources can be geared towards core business functions. Other incentives for utilizing third party vendors include:

- Gain operational or financial efficiencies;
- Increase quality by obtaining specialized expertise;
- Eliminate management problems such as turnover, vacations, etc.;
- Increase availability of services;
- Accelerate delivery of products or services through new delivery channels;
- Increase ability to acquire and support current technology and avoid obsolescence; and,
- Conserve capital for other business ventures.

However, with the gain of the resulting partnerships comes a breeding ground for risk and the need for vendor due diligence.

The Risks

The risks associated with vendor relationships can be unique and vary depending on the service or process outsourced. Some inherent risks associated with utilizing vendor products and services can contribute to operational, legal, and reputational risk. Risk may arise from fraud, error, breach of confidentiality, or the inability to deliver products or services, maintain a competitive position, or manage information.

Other factors in evaluating the quantity of risk at the inception of the vendor process must also be considered. These include:

- Risks pertaining to the business function -
 - Sensitivity of data accessed, protected, or controlled by the vendor;
 - Volume of transactions; and,
 - Criticality to the bank's business.
- Risks pertaining to the vendor -
 - Strength of financial condition;
 - Turnover of management and employees;
 - Ability to maintain business continuity;
 - Ability to provide accurate, relevant, and timely Management Information Systems (MIS);
 - Experience with the function to be performed by the vendor;
 - Reliance on subcontractors;
 - Location; and,
 - Redundancy and reliability of communication lines.
- Risks pertaining to the technology used -
 - Reliability;
 - Security; and,
 - Scalability to accommodate growth.



Breeding Ground for Risk (and Vendor Due Diligence)

Due Diligence

If due diligence and proper controls are not implemented, your bank may face an increased potential for risk. An effective vendor oversight program should provide the framework for Management to identify, measure, monitor, and control the risks associated with doing business with vendors. Your due diligence should address vendor relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the vendor relationship.

In addition to proper due diligence, a good outsourcing relationship should be created. Management can face risks if the relationship with the vendor is not initiated properly and carefully monitored. Good communication should be established early on with your vendors. You should also align your goals and expectations, set clear boundaries, and establish regular dialogue about the relationship and the status. Proper relationship building adds to the win/win situation of utilizing vendors and works to reduce the risks involved.

About the Author: Bobbette Fagel, CISA, CISM

Bobbette is a Certified Information Systems Auditor and Certified Information Security Manager, and has worked with Infotex since its inception. She has been intimately involved in compliance projects for banks and hospitals, and leads our efforts on compliance program development as well as policy and procedure. She handles the reporting aspects of Vulnerability Assessments, Network Architecture Reviews, IT Audits, etc. She has a great understanding of the FFIEC guidelines and stays on top of changes in those guidelines. Bobbette helps clients understand the metrics of risk analysis as well as the business case for information security expenditures (and more importantly, the risk acceptance case for NOT making those expenditures).