Safe Systems

Outsourcing - Rewards and Risks

Tom Hinkel, Director of Compliance

There are twelve booklets in the FFIEC IT Examination Handbook series, and ten of them make reference to the importance of managing third-party relationships. Today, the vast majority of financial institutions outsource at least one business function, and almost 50% of institutions outsource at least one *critical* business function. Among community financial institutions, the percentages are even higher. The two biggest reasons for outsourcing are to cut costs and to gain expertise, but there may be other advantages, such as to increase management focus on core business functions, or to refocus limited internal resources on core functions. Ultimately, the decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Whatever the justification to outsource, institutions are increasingly dependent on their vendors, and the guidance makes it clear that;

> *The responsibility for properly overseeing outsourced relationships lies with the institution's board of directors and senior management.*[1]

And;

> *Financial institutions may outsource some or all of their information processing. Examiners may use this booklet when evaluating the financial institution's risk management process, including the duties, obligations, and responsibilities of the service provider for information security and the oversight exercised by the financial institution.*[2]

In other words, all of the responsibility for maintaining information privacy and security rests with the institution, even though they may have little to no control over the internal processes of the vendor. It is exactly as if the financial institution transferred all of their obligations to the service provider…the same standard of security applies.

> *Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution were conducting the activities in-house*[3]*.*

[1] FFIEC IT Examination Handbook, Outsourcing Technology Services Booklet – June 2004, page 3
[2] FFIEC IT Examination Handbook, Information Security Booklet – July 2006, page 1
[3] FFIEC IT Examination Handbook, Outsourcing Technology Services Booklet – June 2004, page 2

The only difference is that without direct control of the process, it becomes strictly a matter of oversight. The nature and scope of your oversight program will depend on the criticality of the product, service or system to your institutions' operation.

There are three phases in the vendor lifecycle that necessitate the vendor management process, with different expectations and deliverables at each phase:

1. During the vendor selection process, prior to contracting for the product or service
2. After the vendor has been selected, and prior to implementation
3. Post implementation, and ongoing as long as the relationship exists

Once management has determined that the product or service is consistent with their strategic plan, and before the final vendor selection, all potential vendors should undergo a vetting process that should include a review of their financial condition and a reference check. Although the vendor may be reluctant to disclose without a contract, a SAS 70 or other third-party review should be requested if the product or service involves the exchange of non-public customer information.

Once the final vendor selection has been made, the service level agreement (SLA, often included in the contract), should clearly define the expectations on both sides, including respective responsibilities, and remedies in the event of a breach. The "Contract Issues" section of the FFIEC Outsourcing Technology Services Booklet has an excellent summary of everything from scope of service, to duration and dispute resolution.

After implementation, the institution must have a process in place to ensure the vendor delivers the nature and quality of services required by the contract, and that their financial condition gives the institution some measure of assurance that they will be able to continue[4]. Also, since SAS 70 reviews are snapshots of controls at a particular point in time, this report should be requested and reviewed[5] annually, in addition to any other third-party reviews. Additionally, participation in vendor user groups can be advantageous by allowing institutions to discuss concerns and offer input.

The ability to contract for products and services means that even the smallest financial institution can compete with the largest by offering its customers the latest enhanced services, and without the expenses usually associated with hosting in-house. Outsourcing, however, does not reduce the fundamental risks associated with these products and services. Risks such as loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain, and must be addressed though a

[4] The Gladiator Third Party Relationship/Vendor Oversight section of the Information Security Program provides an excellent framework for this process.
[5] Safe Systems has a SAS 70 review flow chart that may assist with this process.

properly designed and implemented vendor management program. The documentation provided by Safe Systems' Quarterly Reviews play an important role in this process, and discussion of vendor management issues (pre-selection, pre-implementation, and on-going) should be a permanent item on your Tech Steering Committee agenda. Safe Systems' customers receive guidance from their account managers as well as our Compliance Department.

About the Author

Tom Hinkel, Director of Compliance, is responsible for ensuring that Safe Systems' services incorporate and abide by appropriate financial industry regulations and best practices. In this position, Hinkel works closely with R&D, Product Management, and Operations Managers to ensure that new and existing services comply with FFIEC standards. Most importantly, by staying current on regulatory issues facing financial institutions, Hinkel serves as a regulatory compliance resource for Safe Systems' customers. With over fifteen years experience, initially on the engineering side installing and supporting bank networks and later in IT regulatory compliance, Hinkel's areas of expertise spans the entire spectrum of information technology. He has served on the inside as Manager of Information Systems, as well as Information Security Officer, and as an independent consultant for banks of all sizes from denovo to $1B+. Hinkel has been with Safe Systems, Inc. since 2005, most recently as an Account Manager. Hinkel holds a Bachelor of Arts degree from Illinois Wesleyan University, an Associate of Arts degree in computer programming, the GSEC security certification from the SANS Institute, and is currently studying towards the Certified Information Systems Auditor designation.

About Safe Systems, Inc.

Founded in 1993, Safe Systems is the national leader in providing compliance-centric IT solutions exclusively to financial institutions. As a technology partner, and recent winner of the MSP Best in Class Award by CompTIA and MSP Partners, Safe Systems has worked with over 500 financial institutions and manages over 16,000 network devices nationwide. Safe Systems' scalable and cost effective solutions include IT managed services, compliance solutions, business continuity and disaster recovery, network design and installation, security services, and IT and compliance training. Safe Systems helps financial institutions to significantly decrease costs, increase revenues, and improve performance. For additional information about Safe Systems, Inc., please visit www.safesystems.com or call 877.752.0550.