Vendor Management – BITS & Pieces

Tom Hinkel, Director of Compliance

FFIEC *Information Systems Examination Handbook*, "Supervision of Technology Service Providers", March 2003

> *A financial institution's use of a [Technology Service Provider] to provide needed products and services does not diminish the responsibility of the institution's board of directors and management to ensure that these activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.*

FFIEC *Information Systems Examination Handbook*, "Outsourcing Technology Services Booklet", June, 2004

> *Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain.*

FFIEC *Information Systems Examination Handbook*," Information Security", July 2006

> *Although outsourcing arrangements often provide a cost-effective means to support the institution's technology needs, the ultimate responsibility and risk rests with the institution. Financial institutions are required under the 501(b) guidelines to ensure service providers have implemented adequate security controls to safeguard customer information.*

The effective management of critical vendors is an essential risk control. The FFIEC mentions this several times in their Examination Handbooks, most recently in the "Information Security" Handbook from July, 2006. Although most financial institutions are accustomed to approaching this from their own perspective, i.e. from the serviced side, I'm going to take a different perspective and approach this issue from our side; the side of the servicer.

As a critical service provider to a financial institution, we respond to requests for information on our compliance with industry information security standards on a frequent basis. Since the guidelines require periodic assessments, we find ourselves responding to the same requests from the same institutions over and over. Each institution seems to require a different set of documentation, and sometimes the required information changes even if the nature of our relationship doesn't. More importantly, we don't always notice an increase in scrutiny if our service level increases. Since the guidelines for reporting are fairly well defined, it would be logical that a standardized format for gathering and disseminating information would be very advantageous, not only to us as the service provider, but also to the financial institution.

Additionally, the biggest challenge for the institution is not getting the actual information, but making sense of it once they have it. SAS 70s, financial statements and recovery procedures are all quite different. Internal auditors can help analyze the financials, but probably aren't much help with IT recovery procedures. Network administrators understand the nuts and bolts of network recovery, but probably can't analyze a SAS 70.

Fortunately, there is a standard resource that may provide the necessary framework. It's called the BITS Standardized Information Gathering Questionnaire. The questionnaire is a tool developed by the BITS consortium, a group of sixty financial industry firms, that is designed to replace the repetitive, labor-intensive process of data collection with a standardized, non-repetitive, labor-saving approach. It is designed to align with multiple industry standards, such as ISO 27002:2005, PCI DSS and COBIT, as well as FFIEC Guidance. The IT Examination Handbook mentions the BITS shared assessment as an example of an industry standard in vendor management. The assessment addresses twelve areas of information security management:

- risk management
- information security policy
- organization of information security
- asset management
- human resources security
- physical and environmental security
- communications and operations management
- access control
- information systems acquisition
- development and maintenance
- information security incident management
- business continuity management
- compliance

The advantage to the service provider is obvious; once the assessment is completed, it can be provided to all requests for a risk assessment- a single, standards-compliant deliverable. From the bank's perspective, it is much easier to analyze and assess information presented in a common format. It's important to note that even though the BITS format gathers all relevant information into one place, it does not relieve the institution from the responsibility of evaluating the information. In other words, the assessment may state that the service provider has completed a SAS 70 review, but the institution should still acquire and review the SAS 70. The assessment organizes the controls in a common format, but the burden of responsibility resides with the financial institution to assess whether or not the controls are adequate given the nature of the institution's relationship to the service provider.

As a critical service provider, Safe Systems is actively engaged in the process of documenting compliance with industry standards regarding information security. The SAS 70 (expected to be complete early Q4) is one of these efforts. We're also evaluating the BITS assessment to determine if this format offers any advantage to our customers, and if so, we'll adopt the format. In the meantime, don't be surprised if one of your service providers offers the BITS assessment the next time you ask for their risk management support documents.

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.