



How to select an information systems audit and security professional services firm for your community bank

www.bankerwatchdog.com

How to select an information systems audit and security professional services firm for your community bank

Industry experience, technical competence, and communication skills are keys to quality service

The need for information systems audit and security services

As identity theft and cyber crimes escalate and receive increased media coverage, the need to secure data is an increasingly daunting challenge for community banks. Likewise, the issue has not escaped the attention of regulators who are heightening their scrutiny of community banks' information security and audit practices. Now more than ever, community banks need to ensure that their information systems (IS) auditors and IS security consulting firms are up to the task at hand.

Selecting or making a transition to a new information systems audit and security firm can be a source of anxiety for community bank executives and audit committees. Concerns about meeting regulatory standards are more prevalent than ever. Concerns about reputation risks from negative, potentially devastating publicity stemming from an information security breach are increasingly on the rise. Not only is technology rapidly changing, but information risks are evolving as well, creating considerable disconcertment to community banks when evaluating IS auditors and information security consultants.

Much of the confusion can be managed and many of these concerns can be mitigated, but it requires research, planning, a little education, and certain proactive steps. The result of this effort can be a productive and cooperative relationship with a firm that understands not only information systems risks, but also understands the business of community banking.

Avoiding problems up front

The criteria used to evaluate a potential firm should include knowledge of banking systems, technical competence, and fees appropriate to the value delivered. The firm's people should be knowledgeable of banking applications to the extent they have a clear understanding of how critical data is stored, transmitted, and processed. This knowledge provides them the ability to identify and articulate true information security risks in the banking environment.

Ideally, community banking should be an area of expertise for the firm versus something they dabble in. Technical competence is a must. This competence can be initially assessed by the relevant certifications held by the firm's team. Vendor-independent certifications such as Certified Information Systems Auditor (CISA) and the National Security Agency's (NSA) Information Assessment Methodology (IAM) and Evaluation Methodology (IEM) are excellent indicators of technical competence. The firm's team should represent an adequate combination of depth and breadth to meet the bank's needs.

The fees charged should reflect the value the firm is able to provide. Value can be assessed based on their ability to identify IS related business risks, to quantify their significance and to make recommendations to improve or enhance IS security.

These criteria can help the bank avoid common problems including:

- Poor service
- Inadequate scope
- Poor mitigation advice
- Regulatory and compliance problems
- Price too high for value received
- High turnover
- Lack of continuing education

Engaging an unqualified IS audit and security firm raises business risks to a community bank. An undiscovered vulnerability is an unmitigated vulnerability that exposes the bank to on-going harm. What if the significance of a risk is poorly quantified? The bank may spend excessively, mitigating certain risks, while remaining exposed on vulnerabilities that pose a bigger, potentially negative impact on the bank's business operations.

These issues can be difficult to correct once a firm is engaged. A diligent selection process helps ensure that unqualified or overpriced firms are not considered and the firm you do choose will add value by meeting or exceeding your expectations.

How to select an information systems audit and security firm

The selection process

Contacting other community banks is always a good place to start. You can also use an Internet search engine to identify firms that offer information system audit and security services in your area. Many will post their qualifications and credentials on their Web site. Seek out firms with a clear focus on these services. Do information system and audit services appear prominently on their Web site? Are their qualifications and credentials clearly stated? Avoid contracting with firms that do not meet these criteria so that your time is used efficiently.

Once firms with the basic criteria are identified, then you may want to research the following:

- Time the firm has been in business
- Affiliations with other organizations
- Qualifications of key personnel
- Litigation history, if available
- Any media coverage related to the firm
- Affiliate memberships in related trade organizations
- Reputation with the banking community

Firms that remain in the running after this step should be contacted for face-to-face meetings.

You should seek to narrow the field to no more than three or four carefully selected firms. Meetings with these firms and selection team should be scheduled. In these meetings the selection team should evaluate the following:

How knowledgeable is the staff of community bank information systems?

A working knowledge of community banking information systems is essential. Can they comfortably discuss, for example, on-line banking, ACH, item processing, and merchant capture?

How will the firm value a bank of your size?

Inquire what size bank and engagement fits within their sweet spot. For an expectation of quality service, your bank and the services you require should fit their profile.

How effective are their communication skills?

Likeability, sense of humor, and communication skills are important in long term relationships. The firm's representatives should present a professional, personable, and approachable demeanor.

How well do they articulate technology issues into business terms?

The firm's ability to effectively relate an audit finding or security vulnerability to a business risk will save the bank time and money in mitigation investments. Most community bank executives have minimal understanding of technical jargon and acronyms. The firm's staff should have the ability to speak about technology in clear and commonly understood business terms.

Do they clearly understand relevant regulatory and compliance requirements?

They should speak comfortably and convey strong knowledge related to FFIEC, GLBA, BSA, and NACHA. The bank should expect to learn of technology related regulatory or compliance issues that may exist from the firm's reporting -- prior to the issues being raised by a regulatory bank examiner.

Do they have adequate resources to provide optimal service to your bank?

The firm's staff should hold vendor-neutral certifications related to information systems audit and security that require continuing professional education (CPE) credits. They should have adequate staff to service their clients. Inquire about key staff longevity and turnover history. The staff should have availability to accommodate your scheduling requirements and be adept in utilizing network security tools.

Narrowing the field

Based on the information the selection team gathers, you should be able to narrow the field to an "A-list". The A-list firms should be invited to submit proposals and given a reasonable amount time to submit their proposals. Firms that value your business will deliver the proposal on or before the deadline.

How to select an information systems audit and security firm

The proposal should be consistent with what you were told during the initial meeting. There should be no unpleasant surprises. Pay special attention to scope, staff assignment, and fee structure.

The proposal should include at least three client references. These references should reflect banks similar in size to your bank that have used the firm for IS audit or other security-related services. Develop a list of questions before contacting the references. Be mindful that the firm selected these references to put the firm in the best possible light. One of your questions should be, “Do you know any other banks that use firm ABC?” Contacting banks that were not included in the proposal will provide a more balanced assessment of the firm’s performance.

Final selection

Additional interviews may be scheduled to address any additional questions or concerns. Fees should be considered in light of the bank’s needs and the firm’s ability to deliver. Be mindful the best firms are likely to have qualified staff, tools, and established processes to support quality service. This commitment to quality represents a significant, on-going investment for the firm, which you should expect to be reflected in the fees. The fees should be competitive and in alignment with the commitment to quality delivery.

Beware of firms that assert high levels of competence and capabilities, but with substantially lower fees than their competitors. This inconsistency is a potential warning sign that the firm is using bait and switch tactics, or that they are making claims of service they are not equipped to deliver.

When the decision does come down to two outstanding firms, fees are sometimes the tie-breaking factor. If both firms have represented themselves fairly, there is not likely to be a major deviation in fees. In the interest of ensuring that you select the best firm for your bank, revisit other important qualifications and intangibles such as personality. Hopefully, you’ll work with the same firm for many years, so the relationship factor will be important.

Timing

The firm should perform IS audit and security projects with enough time allowed to mitigate discovered regulatory or

compliance issues prior to official regulatory examinations. Due to the changing nature of technology, even the best banks will have information systems audit findings and security vulnerabilities discovered. Timely mitigation of issues is an attribute of a bank that is diligent in securing information system assets. The urgency with which the bank mitigates issues may increase the examiner’s confidence in the bank’s information security controls.

Documentation

The firm you select will provide you a list of requested documentation. Depending on the scope of the work, some of these documents will likely be requested:

- Board of director minutes
- IS strategic plan
- IS steering committee charter
- IS steering committee minutes
- Organizational chart
- Key IS job descriptions
- Key IS staff bios
- GLBA 501(b) information security plan
- Disaster recovery and business continuity plan
- Penetration test reports
- Network diagram
- NACHA audits
- Risk assessments
- Key IS vendor contracts
- Key IS third party SAS 70s

This is not intended to represent an all-inclusive list.

Staff

To support a smooth process, you will need to enlist cooperation from within the bank. People you will likely need to designate as resources include:

- Chief financial officer
- Top information systems executive (CIO, IS director, IS manager)
- Network security administrators
- Application security administrators (Core Banking, On-line Banking, Wire Transfer)
- Compliance officer
- Deposits and loan operations managers

How to select an information systems audit and security firm

Take the selection of your IS auditors and information security consultants as seriously as you would any decision that could impact the integrity and reputation of your bank. Now more than ever, you can't afford to increase your risk by using unqualified or inexperienced professional service providers.

The money you spend for IS audit and consulting is an investment -- not only in the safety of your bank's information assets, but in your peace of mind as well. You never want to look back and wonder if you did all you could to protect your bank and your customers from IS-related risks.



About the author

Steve Lineberry, CISA, NSA-IAM, IEM, is the director of IS Assurance & Consulting Services with Nashville-based KraftCPAs PLLC. With over 20 years of experience in information systems management, security and IS risk management, Steve leads KraftCPAs' IS audit team.

A member of the firm's banking industry group, he is responsible for managing FFIEC exams, IS audits, and IS security testing for community banks and other financial institutions. His technical expertise includes Windows, AS/400 and various versions of UNIX. Steve has extensive experience with many core-banking applications including Jack Henry, Fidelity, Metevante, and FISERV.

Steve is a Certified Information Systems Auditor (CISA). This certification program is devoted exclusively to the field of information systems audit, control and security. In addition, Steve holds the National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM) certifications. IAM and IEM are methodologies developed by the National Security Agency for conducting security assessments and evaluations of the critical components of a network.

Steve also teaches classes on information security and audit and has co-authored a book on these subjects. An article, written by Steve, "The Human Element: The Weakest Link in Information Security," was published by the American Institute of Certified Public Accountants in *The Journal of Accountancy*.

About KraftCPAs

Nashville-based KraftCPAs PLLC (www.kraftcpas.com) is a recognized leader in serving the financial and IS needs of community banks. Founded in 1958, KraftCPAs now has over 140 professionals and serves community banks throughout the southeast. KraftCPAs banking industry team provides not only traditional audit and tax services, but a wide range of consulting services, including, but not limited to: FFIEC exams, penetration testing, IS security training, computer network design and set-up, assistance in selecting core processing systems, start-up assistance, Sarbanes-Oxley consulting and implementation, internal auditing, compliance testing and training, loan reviews, assistance with mergers/acquisitions, preparation of regulatory reports, and SAS 70 audits.

KraftCPAs banking industry team has professionals with a variety of expertise, who are dedicated exclusively to the banking industry practice. Certifications held by members of the banking industry team include:

- Certified Public Accountant
- Certified Financial Services Auditor
- Chartered Bank Auditor
- Certified Internal Auditor
- Certified Regulatory Compliance Manager
- Certified Information Systems Auditor

KraftCPAs is an independently owned member of the RSM McGladrey Network – the largest and fastest growing affiliation of quality CPA firms in the United States, Canada and Puerto Rico. This affiliation gives KraftCPAs and its clients resources similar to those of a national CPA firm, coupled with the quality service that is uniquely Kraft.

KraftCPAs was recognized by Goldline Research as one of *The 10 Most Dependable Accounting Firms in the Southeast* (list published in *FORTUNE* magazine, February, 2008 issue). KraftCPAs ranked in the 99th percentile, compared to other CPA firms, in the category of overall client satisfaction on a recently conducted third-party survey. The firm ranked in the 100th percentile, setting new record high scores, in the categories of responsiveness and overall communication.