Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-121-2004
November 16, 2004

Computer Software Due Diligence

Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance

Summary: The FDIC is issuing guidance to financial institutions on performing proper due diligence when selecting computer software or a service provider. This due diligence includes making sure that the software or service provider is compliant with applicable laws, including the Bank Secrecy Act, which includes the USA PATRIOT Act.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Officer

Related Topics:
FFIEC Development and Acquisition Handbook, issued April 2004
Risk Management of Outsourced Technology Services, issued in FIL-81-2000 on November 29, 2000

Attachment:
None

Contact:
Contact Kathryn M. Weatherby, Examination Specialist, at KWeatherby@fdic.gov or (202) 898-6793

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2004/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342 or 202-416-6940).

Highlights:

- The FDIC has determined that certain software products used by financial institutions do not comply with applicable laws and regulations, including the Bank Secrecy Act, which includes the USA PATRIOT Act.
- Management is responsible for ensuring that commercial off-the-shelf (COTS) software packages and vendor-supplied in-house computer system solutions comply with *all* applicable laws and regulations.
- The guidance contained in this financial institution letter will assist management in developing an effective computer software evaluation program to accomplish this objective.
- An effective computer software evaluation program will mitigate many of the risks – including failure to be regulatory compliant – that are associated with software products throughout their life cycle.
- Management should use due diligence in assessing the quality and functionality of COTS software packages and vendor-supplied in-house computer system solutions.

Computer Software Due Diligence
Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance

The FDIC is issuing guidance to financial institutions on performing proper due diligence when selecting computer software or a service provider. This due diligence includes making sure that the software or service provider is compliant with applicable laws, including the Bank Secrecy Act, which includes the USA PATRIOT Act.

The Federal Deposit Insurance Corporation (FDIC) is issuing new guidance for bankers on performing proper due diligence when selecting a software package or service provider, including ensuring that the software package is compliant with applicable laws. The FDIC has identified various Bank Secrecy Act and Anti-Money Laundering (BSA/AML) software products used by financial institutions that do not comply with applicable laws and regulations. Financial institution management is reminded of its responsibility for selecting appropriate computer software products and the need for those products to be compliant with laws and regulations. Software due diligence is critical because of advances in integrated computer systems, remote access to third-party systems, and regulatory changes. As the banking software industry continues to mature, due diligence becomes increasingly critical. Third-party COTS[1] software and vendor-supplied in-house computer system solutions provided by various manufacturers have become crucial components of financial institutions' operating systems. Management should assess the quality of the COTS software packages and vendor-supplied in-house computer systems used by their financial institution. There are essentially two approaches to assure product quality:

1. Validating the process by which the product has been developed; and
2. Evaluating the quality and functionality of the final product.

Assurance of the Selected Product

Selecting and evaluating potential products involve analysis of both the benefits and risks to the existing computer systems, as well as the operating efficiencies of the financial institution. The risks to the operational capability of the existing system must be carefully analyzed. The analysis should include factors such as compliance risk, technical risk, legal risk and security risk. Any approach to product selection should be based on a planned, disciplined and documented methodology.

Assurance of Product Quality

The quality of computer software should be *evaluated and confirmed prior to purchase*. In order to provide quality assurance, management should perform the following steps at a minimum:

- Identify the specific function of the product;
- Identify areas where the product does not meet selection criteria and/or where action plans may be necessary;
- Determine the risks associated with each criteria not met by the product;
- Document how the financial institution will mitigate or alleviate those risks;
- Obtain a list of current users and contact users;
- Implement selected system(s) in a test mode and fully test the system to ensure all requirements are met;
- Determine product security and the potential impact to the operation if that security is breached; and
- Evaluate the support for the products, including the vendor's stability, product strategy, support record and update policy.

Final Product Quality

Ineffective product utilization can lead to breakdowns during initial development as well as throughout the life cycle of a software product line. Major risks include:

- *Unknown interactions.* There may be unknown interactions between the product components and other components that could result in a system that does not behave as intended.
- *Poor product quality.* Products without extensive track records pose the risk of failing to meet the reliability standards for the system. Failure to adequately qualify or test a product can admit an unacceptable product into the system.
- *Inappropriate product for the job.* Failure to comprehensively qualify a product for its intended usage may result in the selection of a product that fails to meet the quality requirements needed, such as security.

Management is responsible for reviewing, to the extent possible, how the product will function in the financial institution's environment. Management is expected to analyze and document the evaluation of the product.

Regulatory Requirements

Management should include a regulatory requirement clause in its financial institution's licensing agreements for core-processing or mission-critical applications. The clause should require vendors to maintain application software so that the software operates in compliance with all applicable federal and state regulations.

Conclusion

Financial institution management should perform adequate due diligence to ensure that software solutions meet the needs of the institution and function as required by current applicable laws and regulations. The due diligence process must be performed on an on-going basis to ensure that technical software solutions remain compliant if the applicable regulation changes over time. Financial institution management is responsible for complying with all laws, regardless of whether the product or the service provider fails to perform as promised. In addition, if regulations change over time, management is still responsible for compliance, even though computer software and vendor-supplied in-house computer systems may or may not change. Penalties could occur if a bank's systems, programs and controls do not meet regulatory requirements.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection

[1]COTS - Commercial off-the-shelf software products are developed by a third party (which controls its ongoing support) and are ready-made and available for sale to the general public. COTS software normally does not allow modification at the source-code level, but may include mechanisms for customization.