Financial Institution Letters

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

FIL-121-2004
November 16, 2004

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.

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.

Continuation of FIL-121-2004

Frequently Asked Questions

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 FILs 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).

Financial Institution Letters
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

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.

Last Updated 08/18/2005 communications@fdic.gov

Financial Institution Letters

Frequently Asked Questions Received On Financial Institution Letter 121-2004: Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance

- On November 16, 2004, the FDIC issued FIL-121-2004, Computer Software Due Diligence Guidance on Developing an Effective Computer Software Evaluation Program to Assure Quality and Regulatory Compliance. This guidance was issued to assist bank management in developing an effective computer software evaluation program.
- Since the issuance of this guidance, the FDIC has received numerous inquiries from the industry seeking clarification on various aspects of the guidance. The FDIC has provided answers to these questions and is distributing many of these as an attachment to this FIL.
- The frequently asked questions ("FAQ") document is composed of 15 frequently asked questions from the industry, and includes regulatory responses to each question.

1. What software products used by financial institutions do not comply with applicable laws and regulations?

The source of this information is confidential supervisory information, which we are not permitted to disclose. The primary intent of this Financial Institution Letter ("FIL") is to remind management of their due diligence requirement when selecting a vendor or computer software solutions to business problems. Because of new and changing banking laws and implementing regulations, some software vendors, providers of commercial off-the-shelf ("COTS") products and in-house legacy systems may not be fully updated in applying all necessary changes required for compliance. Of particular note are the in-house legacy systems and COTS products, where needs were identified and a product was developed to meet those needs, but the required enhancements to keep the product updated and in compliance were not made.

FIL #121-2004 states, "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 FIL further states, "The due diligence process must be performed on an on-going basis to ensure that technical software solutions remain compliant...."

2. Could you clarify what kinds of applications qualify as core-processing or mission-critical applications? For example, would the following software functions be considered mission critical: software used in network routers to control Virtual Private Networks (VPN), software in an anti-spam appliance, or anti-virus software?

Essentially, core-processing or mission-critical applications are those that provide the foundation for the financial institution to conduct daily business operations. These core-processing or mission-critical applications differ from one financial institution to another. In the case of a retail financial institution, the deposit and loan applications would be considered core-processing and mission-critical applications. For a wholesale bank, loan-generation and secondary-market applications would be considered core-processing or mission-critical applications. An Internet-bank would identify access to the Internet as a mission-critical application, while the core applications would include deposits, checking, and bill payment. An international bank with trust activities would include SWIFT and funds transfer applications as mission critical, while the deposit, loan, secondary market, trust, and security applications (among others) would be core applications.

Typically, software used in network routers would not be considered as a core-processing or mission-critical application as the software is being used to provide a pathway to an application or data. On the other hand, it could be considered mission critical if it were the only router on the system, all access requests were sent through that router, and failure of the router would halt business.

3. Should a bank be able to search its database (electronic records) for multiple criteria such as, a person, business, social security number ("SSN"), address, driver's license number, tax identification number, or any other identifying information?

Yes, it is necessary to maintain the ability to search databases beyond just name and SSN to ensure compliance under the Bank Secrecy Act ("BSA") and the bank's in-house customer identification program ("CIP") as required by Section 326 of the USA PATRIOT Act. Additional information about CIP programs can be found in FIL-90-2004, published July 28, 2004.

4. If a compliance question arises after an application is installed, who is the final arbiter for disputed interpretations of a regulation between a bank and a technology service provider?

These issues are generally addressed in the contract, and typically involve an arbitration process. If they cannot be resolved through this process, the final solution may require a legal interpretation.

5. Why were these guidelines developed? Is the type of software in question used specifically to prevent money laundering or are there broader applications?

The FDIC discovered, through the examination process, that certain software products used by financial institutions do not comply with applicable laws and implementing regulations of the BSA. The products identified by the FDIC that resulted in this guidance were being used to meet BSA compliance; however, management's due diligence requirement extends to all products.

The guidelines were issued to remind bank management of their due diligence responsibilities when selecting vendors and products. Bank management should be aware of their due diligence requirement any time a vendor or product is selected to perform a bank function.

6. When are the guidelines effective? Do they have the force of a legal and/or regulatory mandate?

In general, FILs are used to communicate guidance and are effective when issued. While this guidance provided specific reminders relating to the use of vendor products and software to comply with the BSA regulations, bank management's responsibility has always been to ensure that the bank complies with applicable laws. While the guidance is not a regulatory mandate, following it may improve the institution's compliance with applicable laws and regulations.

7. Has the FDIC identified vendors that produced non-compliant COTS software for the purpose of Bank Secrecy Act compliance?

The FDIC has identified some vendor and software products that are not configured correctly or lack the functionality to retrieve and retain documentation for required regulatory time frames. When products were identified that did not fully comply with the BSA, the bank or vendor initiated corrections immediately.

8. Does the FDIC have similar guidelines for firms that develop their own in-house BSA software rather than purchase a vendor product?

Bank management is responsible to ensure that the bank complies with applicable laws and regulations regardless of whether products are purchased or internally developed.

9. Are these guidelines similar to those that exist for the purchase of software used to monitor the Office of Foreign Assets Control ("OFAC") list?

Yes.

10. Since decisions of this type are normally made by the Department of the Treasury or Federal Financial Institutions Examination Council ("FFIEC"), why did the FDIC issue these guidelines?

The FDIC examination process identified certain BSA and Anti-Money Laundering ("AML") software products used by financial institutions that did not comply with applicable laws and regulations. FIL #121-2004 was a reminder to bank management of its **pre-existing** due diligence responsibility. The FFIEC and Federal Banking Agencies have jointly and individually released guidance to their institutions and/or the industry about risk from third-party products. This issuance is consistent with that practice. The FDIC, as part of its supervisory program of state-nonmember banks, issues guidance to inform institutions of risks and best practices.

11. The FFIEC published guidance on the acquisition of free and open software ("FOSS") on October 21, 2004. Does the FDIC's guidance amend the FFIEC's FOSS guidance?

This guidance does not amend the FFIEC FOSS guidance; it simply offers financial institutions guidance on additional areas of risk identified by the FDIC.

12. Would workstation applications such as Windows XP and Microsoft Office be affected?

These applications would be included if they are core-processing or mission-critical applications that provide the foundation for your financial institution to conduct daily business (refer to response to question #2). Alone, Windows XP and Microsoft Office would themselves not be affected; however, core-processing or mission-critical programs that utilize Windows XP (or a variant thereof) could be affected. These applications vary from one financial institution to another.

13. Would network applications such as virus scan software be affected?

Virus scan software is considered a COTS product. Similar to Windows XP and Microsoft Office, virus scan software may or may not be considered a core-processing or mission-critical application (refer to response to question #2).

14. BSA/AML applications are specifically referenced. Are these the only applications in question?

The due diligence requirement exists for all purchased or internally developed products. Please refer to the response for question #2. Also, as stated in the Conclusion section of FIL-121-2004:

> "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 FIL further states, "the due diligence process must be performed on an on-going basis to ensure that technical software solutions remain compliant...."

15. The guidance refers to a regulatory requirement clause that requires vendors to maintain application software in compliance with all applicable federal and state regulations. Does this mean a software vendor cannot use separate add-on products?

The FDIC recognizes that software packages generally do not meet every regulatory requirement. FIL-121-2004 is intended to provide guidance to financial institutions performing proper due diligence when selecting computer software and/or a service provider. To meet certain reporting and/or processing requirements, compliance can be obtained through other core or add-on products.

Management should confirm and document compliance as part of their due diligence. Due diligence should ensure that each product performs the tasks for which it was purchased, and that the program is in compliance with the laws and regulations associated with those tasks.