



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

Financial Institution Letter
FIL-105-2007
December 4, 2007

INFORMATION TECHNOLOGY – RISK MANAGEMENT PROGRAM

Revised IT Officer’s Questionnaire

Summary: The FDIC has updated its risk-focused information technology (IT) examination procedures for FDIC-supervised financial institutions. As part of the revision, the IT Officer’s Questionnaire was enhanced to provide greater coverage of vendor management and outsourcing topics, credit card and ACH (automated clearing house) payment system risks, and an institution’s overall information security program. The revised questionnaire is attached.

Distribution:

FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:

Chief Executive Officer
Chief Information Officer
Chief Information Security Officer
Chief Compliance Officer

Related Topics:

Interagency Guidelines Establishing Information Security Standards

Uniform Rating System for Information Technology

Attachment:

IT Officer’s Questionnaire

Contacts:

Senior Examination Specialist Donald Saxinger at dsaxinger@fdic.gov or (202) 898-6521

Note:

FDIC financial institution letters (FILs) may be accessed from the FDIC’s Web site at <http://www.fdic.gov/news/news/financial/2007/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 via the FDIC’s Public Information Center (1-877-275-3342 or 703-562-2200).

Highlights:

- The IT Officer’s Questionnaire is an essential element of the FDIC’s information technology examinations of FDIC-supervised financial institutions.
- A “Vendor Management and Service Provider Oversight” section was added to the questionnaire to reflect potential reliance on outside firms for technology-related products and services.
- New questions were added for payment system risks, including questions relating to the Originating Depository Financial Institution (ODFI), wire transfer, credit card merchant processing, and remote deposit capture.
- All questions now include at least one reference to existing guidance or regulations.
- The summary section for Part 364, Appendix B, Interagency Guidelines Establishing Information Security Standards, was replaced with a reference document that maps applicable questionnaire items to the Guidelines. This reference document will assist financial institution management in conducting self-assessments of their information security programs. Evaluating compliance with the Guidelines is part of every IT examination.
- The IT Officer’s Questionnaire must be completed and signed by an executive officer of the financial institution and returned to the FDIC examiner-in-charge prior to the on-site portion of the examination.