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

Financial Institution Letter
FIL-81-2005
August 18, 2005

INFORMATION TECHNOLOGY RISK MANAGEMENT PROGRAM (IT-RMP)

New Information Technology Examination Procedures

Summary: The FDIC has updated its risk-focused information technology (IT) examination procedures for FDIC-supervised financial institutions.

Distribution:
FDIC Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer
Chief Information Officer
Compliance Officer
Legal Counsel

Related Topics:
Interagency Guidelines Establishing Information Security Standards

FFIEC Uniform Rating System for Information Technology (URSIT)

Attachment:
None

Contact:
Donald Saxinger
Technology Supervision Branch
(202) 898-6521

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2005/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's new risk-focused IT examination procedures focus on the financial institution's information security program and risk-management practices for securing information assets.
- The IT Examination Officer's Questionnaire must be completed and signed by an officer of the financial institution and returned to the FDIC examiner-in-charge prior to the on-site portion of the examination.
- The new examination procedures apply to all FDIC-supervised financial institutions, regardless of size, technical complexity or prior examination rating.
- IT examination findings and a single IT "composite" rating will be included in the consolidated Risk Management Report of Examination.

INFORMATION TECHNOLOGY RISK MANAGEMENT PROGRAM (IT-RMP)
New Information Technology Examination Procedures

On June 30, 2005, the Federal Deposit Insurance Corporation (FDIC) implemented a new Information Technology Risk Management Program (IT-RMP) for conducting IT examinations of FDIC-supervised financial institutions. IT-RMP examination procedures apply to all FDIC-supervised banks, regardless of size, technical complexity or prior examination rating. The former IT-MERIT (Maximum Efficiency, Risk-Focused, Institution Targeted) procedures and related work programs have been rescinded.

IT-RMP procedures focus on the financial institution's information security program and risk-management practices for securing information assets. These risk-management practices include:

- Risk assessment,
- Operations security and risk management,
- Audit and independent review,
- Disaster recovery and business continuity, and
- Compliance with Part 364, Appendix B of the FDIC's Rules and Regulations.

IT examination findings will be reported in the consolidated Risk Management Report of Examination. A single "composite" IT rating will be assigned as defined by the Uniform Rating System for Information Technology (URSIT). Including the IT examination findings and rating in the Risk Management Report will serve to highlight the relationship between business-related risk-management practices and technology-related risk-management practices. Key features of the IT-RMP include:

- IT Examination Officer's Questionnaire. This questionnaire covers the risk-management practice areas listed above and will serve as both a pre-examination scoping tool and on-site examination tool by examiners. The questionnaire must be completed and signed by an officer of the financial institution and returned to the examiner-in-charge prior to the on-site portion of the examination. The questionnaire solicits responses primarily in a "Yes/No" format with space for optional narrative comments.

- Flexible use of work programs. Using the risk-management practice categories in the IT Examination Officer's Questionnaire, examiners may streamline or expand on-site examination activities as needed using applicable FDIC- or FFIEC-approved work programs, FDIC Financial Institution Letters or other regulatory guidance.

- Pre-examination Request List. The IT Examination Officer's Questionnaire is the only mandatory pre-examination documentation requirement. Examiners may, at their discretion, request additional information to expedite on-site examination activities.

- IT Rating Guidelines. Only a composite IT assessment rating will be assigned. The rating will be based upon the existing URSIT definitions. Component IT ratings will no longer be assigned.

For further information about the FDIC's new IT examination procedures, please contact your FDIC Division of Supervision and Consumer Protection Regional Office. Please share this information with your Chief Information Officer.

Michael J. Zamorski
Director
Division of Supervision and Consumer Protection