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

Financial Institution Letter
FIL-43-2016
June 30, 2016

Information Technology Risk Examination (InTREx) Program

Summary: The FDIC updated its information technology and operations risk (IT) examination procedures to provide a more efficient, risk-focused approach. This enhanced program also provides a cybersecurity preparedness assessment and discloses more detailed examination results using component ratings.

Statement of Applicability to Institutions with Total Assets Under $1 Billion: This Financial Institution Letter applies to all FDIC-supervised institutions.

Distribution:
FDIC Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer
Chief Information Officer

Related Topics:

FIL-28-2015 *FFIEC Cybersecurity Assessment Tool*

FIL-22-2001 *Security Standards For Customer Information*

Part 364 Appendix B - *FDIC Rules and Regulations*

FIL-12-1999 *FFIEC Uniform Rating System for Information Technology (URSIT)*

Attachments:

InTREx Program

Contacts:
Rookmatie Veerasammy, Information Technology Section, 703-254-0832 rveerasammy@fdic.gov

Henry Jumonville, Information Technology Section 703-254-2235 hjumonville@fdic.gov

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at https://www.fdic.gov/news/news/financial/2016/.

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

Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877-275-3342 or 703-562-2200).

Highlights:

- The InTREx Program is an enhanced, risk-based approach for conducting IT examinations. The Program helps to ensure that financial institution management promptly identifies and effectively addresses IT and cybersecurity risks.
- All Uniform Rating System for Information Technology (URSIT) component and composite ratings assigned at each IT examination will be included in the Risk Management Report of Examination.
- An assessment of the financial institution's cybersecurity preparedness will be included on the Information Technology and Operations Risk Assessment Page of every Risk Management Report of Examination.
- The InTREx Program includes a streamlined IT Profile that financial institutions will complete in advance of examinations that replaces the IT Officer's Questionnaire (ITOQ). The IT Profile is intended to provide examination staff with more focused insight on a financial institution's IT environment and includes 65 percent fewer questions than appeared on the FDIC's legacy ITOQ.

Financial Institution Letter
FIL-43-2016
June 30, 2016

Information Technology Risk Examination (InTREx) Program

Enhanced Information Technology and Operations Risk Examination Procedures

On July 1, 2016, the Federal Deposit Insurance Corporation (FDIC) implemented the Information Technology Risk Examination (InTREx) Program for conducting information technology and operations risk (IT) examinations of FDIC-supervised financial institutions. The InTREx Program is designed to enhance identification, assessment, and validation of IT in financial institutions and ensure that identified risks are effectively addressed by FI management. FIL-81-2005, *Information Technology Risk Management Program (IT-RMP),* has been rescinded.

InTREx uses a work program based on the Uniform Rating System for Information Technology[1] (URSIT) and includes Core Modules for the Audit, Management, Development and Acquisition, and Support and Delivery component ratings. The Core Modules incorporate procedures to assess compliance with Appendix B to Part 364 of the FDIC Rules and Regulations entitled *Interagency Guidelines Establishing Information Security Standards*[2,3] as well as procedures to assess cybersecurity preparedness. The results of these assessments will be embedded in the Risk Management Report of Examination.

Other features of the InTREx program are:

- Enhanced Pre-Examination Process. The pre-examination scoping process has been revised and streamlined to focus on emerging risks and technologies.
    - Approximately 90 days before a scheduled IT examination, the financial institution will receive an Information Technology Profile (ITP) questionnaire through *FDICconnect* to be completed and returned to the FDIC. The ITP is designed to determine the resources needed to perform the IT examination and assist with scoping the examination. The ITP includes 65 percent fewer questions than the Officer's Questionnaire used in the previous IT examination program.
    - The IT examiner-in-charge will risk focus the IT examination based on responses to the ITP and other available information (e.g., prior examination reports, new products or services, etc.). At least 45 days before the scheduled examination start date, an IT Request Letter reflecting the IT profile of the institution will be sent to the financial institution through *FDICconnect.* Management should upload requested information within the requested time frame to minimize on-site information requests.

[1] See FIL-12-1999 *FFIEC Uniform Rating System for Information Technology (URSIT)* - https://www.fdic.gov/news/news/financial/1999/fil9912.html

[2] See Part 364 Appendix B - *FDIC Rules and Regulations* - https://www.fdic.gov/regulations/laws/rules/2000-8660.html#fdic2000appendixbtopart364

[3] See FIL-22-2001 *Security Standards For Customer Information* - https://www.fdic.gov/news/news/financial/2001/fil0122.html

- Examination Procedures. Examiners will complete the InTREx Core Modules, the Cybersecurity Workpaper, and the Information Security Standards Workpaper to assess risk and to document examination procedures, findings, and recommendations. For financial institutions with a higher IT profile, examiners can use expanded examination procedures, supplemental workprograms, and the FFIEC Information Technology Examination Handbook.

- Report Presentation. A summary of the overall condition of the IT function supporting the URSIT composite rating will be included on the Examiner Conclusions and Comments page. The Information Technology Assessment page will document URSIT component ratings, examination findings, recommendations, management's responses, including timeframes for corrective action, and supporting comments for cybersecurity preparedness and compliance with information security standards.

For further information about the FDIC's revised IT examination procedures, please contact your FDIC Regional Office.

Doreen Eberley
Director
Division of Risk Management Supervision