FDIC Adopts Strong Risk-Focused Approach for IT Exams

The FDIC recently updated its information technology and operations risk examination procedures. Dubbed "Information Technology Risk Examination (InTREx) Program," the Program is designed to enhance the ability of examiners to identify, assess and validate a financial institution's information technology and operations risk and to ensure that institution management is affectively addressing identified risks.

InTREx uses a work program based on the Uniform Rating System for Information Technology (URSIT), which the banking agencies use as a means of uniformly assessing and rating IT-related risks of financial institutions and their third party servicers. Using core modules, FDIC examiners will assign composite ratings for, again based on the URSIT critical components: Audit, Management, Development and Acquisition, and Support and Delivery. The FDIC also has incorporated into the core modules procedures for assessing FDIC-supervised institutions' cybersecurity preparedness, In addition, InTREx includes procedures for evaluating compliance with the Interagency Guidelines Establishing Information Security Standards (Appendix B to 12 CFR Part 364).

The InTREx Program also includes the following components.

- An enhanced pre-examination process designed to streamline the pre-examination scoping process to focus on emerging risks and technologies. In particular, approximately 90 days before a scheduled IT examination, the financial institution will receive an Information Technology Profile (ITP) questionnaire through FDICconnect. The ITP is designed to determine the resources needed to perform the IT examination and assist with scoping the examination. According to the FDIC, the ITP has 65 percent fewer questions than the Officer's Questionnaire currently used for IT exams.

18500 von karman avenue, suite 300, irvine, california 92612
phone: (800) 742-3600 • fax: (949) 474-0617
email: bcg@ablawyers.com • website: www.bankerscompliancegroup.com

The IT examination will be based on responses to the ITP and other available information, such as 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. FDIC notes that management should upload requested information within the requested time frame to minimize on-site information requests.

- In assessing IT risk and to document examination procedures, findings and recommendations, examiners will complete the InTREx core modules, the cybersecurity workpaper and the information security standards workpaper. Examiners also may use expanded examination procedures, supplemental workprograms, and the FFIEC Information Technology Examination Handbook for financial institutions that have a high IT profile.

- Examiners will provide a summary of the overall condition of the IT function supporting the URSIT composite rating. This summary 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.

Information regarding the InTREx Program, including the core modules, was made a part of FDIC FIL-43-2016, which can be downloaded from the FDIC's website at **www.fdic.gov/news/news/financial/2016/fil16043.html**.