TEXAS DEPARTMENT OF BANKING

★ *Dedicated to Excellence in Texas Banking* ★

SUPERVISORY MEMORANDUM – 1020

August 7, 2018

TO: All State-Chartered Banks, Trust Companies, and Technology Service Providers; and All Bank and Trust Examining Personnel

FROM: Charles G. Cooper, Banking Commissioner

SUBJECT: Information Technology Examination Frequency and Ratings[1]

PURPOSE

This Supervisory Memorandum sets forth the Information Technology (IT) examination ratings and frequency guidelines for banks, trust companies, and technology service providers. The three types of examination scopes utilized by the Department for IT reviews are also defined in this policy.

IT EXAMINATION RATINGS

Banks and Trust Companies

The Department will issue component and composite ratings at each full scope examination for banks and trust companies. The overall rating is determined based on a review of IT risk-focused examination work procedures centered on managerial oversight including: establishment of policies and procedures; assessment of IT risks; testing of key controls; providing for business continuity after a disaster; and safeguarding of customer information. Component ratings are assigned for Audit, Management, Development & Acquisition, and Support & Delivery. Financial institutions under the continuous supervision examination program have component ratings issued along with the composite rating. The component and composite rating practices are addressed in Supervisory Memorandum 1001.

Technology Service Providers (TSPs)

The Department issues component and composite ratings for TSPs. The focus for the review is on four functional IT component areas: Audit, Management, Development & Acquisition, and

---

[1] This policy was revised to remove references to Level I and Level II IT examination scopes. The Level II examination scope is no longer utilized with the implementation of the Information Technology Risk Examination (InTREx) Program. Additionally, the policy was revised to clarify that both component and composite ratings will be issued at each Full Scope examination; clarify the definition of a Tier 3 Technology Service Provider; and remove the IT Examination Scope and Frequency tables for state-chartered banks and trust companies to avoid duplication of existing content within this policy.

Support & Delivery. The component and composite rating practices, as established in Supervisory Memorandum 1001, apply to TSPs.

SCOPE OF EXAMINATIONS

The scope or depth of each IT review will be determined based on the assessed IT risks of each institution as directed by the Director of IT Security Examinations (DITSE) or the Chief IT Security Examiner (CITSE). The Department utilizes three types of examination scopes for IT reviews: Full Scope, Visitation, and Continuous.

- A Full Scope Examination (Full Scope) is the most comprehensive. Examiners complete procedures that are designed to assess the entity's IT risks and controls. Component ratings and an overall composite rating will be issued and included in a Report of Examination produced for the entity.

- A Visitation is a narrowly scoped examination which may focus on one or more specific risk areas. The results of a Visitation will be documented with a Letter of Findings to the entity.

- A Continuous Examination Program (CEP) is primarily utilized in larger institutions, generally $10 billion and greater or as determined by the Commissioner or Deputy Commissioner and includes a series of targeted reviews conducted over an examination cycle generally covering a 12-month period. The targeted reviews focus on one or more specific areas of the institution's IT operations. The results of targeted reviews are documented in a Letter of Findings. The results of the IT targeted reviews performed during the examination cycle are utilized to assign a composite CAMELS rating for the institution which is documented in a Report of Examination.

The Full Scope and CEP examinations meet the examination priorities of the Department and federal regulators. As with any functional area of a financial institution, if there are supervisory concerns about IT related risks, then interim examinations, on-site visits, and off-site monitoring may be performed as recommended by the DITSE or CITSE in collaboration with the applicable Regional Director (RD) or Chief Trust Examiner (CTE). These reviews and scope determinations will be performed under the direction of the DITSE or CITSE who can expand the scope of the examination when necessary.

The findings of the IT examinations may be embedded into the safety and soundness Report of Examination for the institution or delivered under separate cover as an independent Report of Examination or Letter of Findings as determined by the DITSE or CITSE and applicable RD or CTE.

EXAMINATION FREQUENCY

State-Chartered Banks

The frequency of an IT examination *generally* follows the frequency of safety and soundness examinations for state-chartered banks. IT examinations generally will be scheduled within 120 days prior to, or on the same day as, the start date of the safety and soundness examination. In certain circumstances, the examination may be delayed up to 60 days after the safety and soundness

examination start date, with the concurrence of the Director of Bank and Trust Supervision. The frequency of safety and soundness examinations for state-chartered banks is addressed in Supervisory Memorandum 1003.

In situations where the most recent composite IT rating is 3, 4 or 5, the IT examination frequency will continue to coincide with the safety and soundness examination frequency; however, during the interim, a Full Scope examination, Visitation, or an Off-site review will be performed 90 days before or 90 days after the mid-point in the safety and soundness examination cycle. The scope and timing of the interim examination will be determined by the DITSE or CITSE based on factors such as severity of weaknesses, management's capability, and information in progress reports. Component and composite IT ratings will be assigned at a Full Scope examination and a Report of Examination will be provided to the bank. If a Visitation or Off-site review is performed, then no rating will be assigned, and a Letter of Findings will be provided to the bank.

Exceptions to the IT Examination Frequency for State-Chartered Banks

Change in Scope of Safety and Soundness Examination

If the safety and soundness Interim Risk Examination and Assessment (IREAP)[2] examination is converted to a Level I Full Scope examination and the Bank Composite Rating is subsequently upgraded to allow for an 18-month examination cycle, then:

(1) If the IT Rating is a 1 or 2:

- A Full Scope IT exam will be performed approximately 6 months after the converted Full Scope safety and soundness exam. The IT examination frequency will then follow the 18-month cycle; or

(2) If the IT Rating is a 3, 4, or 5:

- A Full Scope IT examination will be performed approximately 6 months after the converted Full Scope safety and soundness examination followed by a Full Scope IT examination, Visitation, or Off-site review in 12 months. The IT examination frequency will then follow the 18-month cycle with a Full Scope examination, Visitation, or an Off-site review performed 90 days before or 90 days after the mid-point in the safety and soundness examination cycle.

Change in Frequency of Safety and Soundness Examination

In the event the financial institution's safety and soundness examination frequency increases, if the most recent IT composite risk rating is a 1 or 2, then the IT examination may be delayed up to 6 months after the safety and soundness examination due date.

If the safety and soundness examination is delayed for any reason, the IT examination may be delayed as well with the goal of beginning the IT examination no later than during the safety and soundness examination. The flexible due date allows coordination with the bank to reduce regulatory burden, to preclude conflicts with safety and soundness examination procedures, and to

[2] The Interim Risk Examination and Assessment Program (IREAP) is defined in Supervisory Memorandum 1003.

provide the option for the IT examination information to be collected closer to the date of the safety and soundness examination.

Trust Companies

The frequency of an IT examination generally follows the frequency of safety and soundness examinations for trust companies, with the IT examination due within 120 days prior to or on the same say as the start day of the trust company examination. In certain circumstances, the examination may be delayed up to 60 days after the safety and soundness examination start date, with concurrence by the Director of Bank and Trust Supervision. Trust companies exempt under Texas Finance Code §182.011, do not receive an IT examination. The frequency of safety and soundness examinations for trust companies is addressed in Supervisory Memorandum 1004.

In situations where the most recent composite IT rating is 3, 4 or 5, the IT examination frequency will continue to coincide with the safety and soundness examination frequency; however, during the interim, a Full Scope examination, Visitation, or an Off-site review will be performed 90 days before or 90 days after the mid-point in the safety and soundness examination cycle. The scope and timing of the interim examination will be determined by the DITSE or CITSE based on factors such as severity of weaknesses, management's capability, and information in progress reports. Component and composite IT ratings will be assigned at a Full Scope examination and a Report of Examination will be provided to the trust company. If a Visitation or Off-site Review is performed, then no rating will be assigned, and a Letter of Findings will be provided to the trust company.

Exceptions to the IT Examination Frequency for Trust Companies

Change in Frequency of Safety and Soundness Examination

In the event the trust companies' safety and soundness examination frequency increases, if the most recent IT composite risk rating is a 1 or 2, then the IT examination may be delayed up to 6 months after the safety and soundness examination due date.

If the safety and soundness examination is delayed for any reason, the IT examination may be delayed also, with a goal of beginning the IT examination no later than during the safety and soundness examination. The flexible due date allows coordination with the trust company to reduce the regulatory burden, to preclude conflicts with safety and soundness examination procedures, and to provide the option for the IT examination information to be collected closer to the date of the safety and soundness examination.

Technology Service Providers (TSPs)

TSPs are assigned to one of three examination frequency tiers by the DITSE or CITSE. The tier assigned to each TSP will be based on a variety of factors including complexity of the TSP, the number of state-chartered banks and trust companies that they service, the type of information technology service they provide, their affiliation with state-chartered institutions, and if they are subject to examination by other regulatory agencies.

The three tiers are defined as follows:

Tier 1

These TSPs are generally owned, controlled, or otherwise affiliated with a bank that provides critical data processing and/or managed services for affiliated banks. Tier 1 TSPs will be examined on a frequency as determined by the FFIEC Risk-Based Examination Priority Ranking in the Federal Regulatory Agencies' *Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers.* The FFIEC Risk-Based Examination Priority Ranking form will be completed at the conclusion of each IT examination of a TSP. For 1 and 2 rated Tier 1 TSPs, the DITSE or CITSE may establish more frequent examinations than as determined by the Examination Priority Ranking as long as the frequency is not more often than the safety and soundness examination of the lead affiliated bank. (Often TSPs and their affiliated banks share IT control policies and procedures. Conducting an IT examination of the TSP that coincides with IT examinations of the affiliated banks can result in a substantial reduction in regulatory burden.)

In situations where the most recent composite IT rating is 3, 4 or 5, the examination frequency will follow the FFIEC examination frequency; however, during the interim, a Full Scope or Visitation examination may be performed. The scope and timing of the interim examination will be determined by the DITSE or CITSE based on factors such as severity of weaknesses, management's capability, and information in progress reports.

The findings of TSP examinations will be conveyed through an IT Report of Examination.

Tier 2

These TSPs are generally companies such as large national data processing companies that are included in the FFIEC's Significant Service Providers (SSP) Program, formerly referred to as the Multi-Regional Data Processing Servicers (MDPS) Program. Tier 2 TSPs are examined by FFIEC member agencies under a prescribed frequency and are not subject to routine examination by the Department, although staff may participate in the examination of these entities with federal agencies. Due to the type of service they provide and number of banks they service, the Department monitors examination data received from the FFIEC member agencies.

Tier 3

These TSPs are often small regional technology services companies or companies that primarily provide secondary technology services to state-chartered financial institutions. Secondary technology services are primarily non-core data processing services such as document imaging, item processing, credit reporting, statement rendering, and compliance reporting. Tier 3 TSPs are generally examined by FFIEC member agencies. Department staff may participate in the examination of these entities with federal agencies, elect to conduct an independent examination based on the risk profile of the TSP, or defer to the FFIEC agencies. The Department monitors examination data received from the FFIEC member agencies on Tier 3 TSPs.

COOPERATIVE EXAMINATION PROGRAM – BANKS AND TECHNOLOGY SERVICE PROVIDERS

The Department of Banking in cooperation with the Federal Reserve Bank of Dallas (FRB) and the Federal Deposit Insurance Corporation (FDIC), has committed to coordinating examination

efforts to reduce regulatory burden. As a result, the general practice of the agencies is to alternate examinations between the Department and the FDIC or, if the institution is a member bank, with the FRB. However, the Department will conduct a separate examination, or a joint examination with the appropriate federal supervisory agency, whenever deemed appropriate. IT examinations of commercial banks performed by federal banking agencies will be accepted in meeting the Department's examination priority guidelines.

CONTACT INFORMATION

Questions about this policy may be directed to either Kurt Purdom, Director of Bank and Trust Supervision, at 512-475-1300, or the Department's Chief IT Security Examiner, Ruth Norris, at 713-932-6146.