



TEXAS DEPARTMENT OF BANKING

★ *Dedicated to Excellence in Texas Banking* ★

SUPERVISORY MEMORANDUM – 1020

March 15, 2016(rev.)

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 Ratings¹

PURPOSE

This Supervisory Memorandum (Memorandum) sets forth the Information Technology (IT) examination frequency guidelines for banks, trust companies, and technology service providers. The Memorandum also addresses which entities receive individual component ratings for IT examinations and which receive only an overall composite rating. The four types of examination scopes utilized by the Department for IT reviews are defined in this policy.

This policy has been revised to update the IT examination scope and frequency table for state-chartered banks. The table was revised as follows: (1) banks with total assets of \$10 billion or greater qualify for a continuous examination program; and (2) banks with total assets of \$1 billion or less may qualify for an 18 month examination cycle.

IT EXAMINATION RATINGS

Banks and Trust Companies

In general, the Department issues only an overall composite IT rating 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. Banks under the continuous supervision examination program, however, may have component ratings issued along with the composite rating.

¹ This Supervisory Memorandum supersedes the March 19, 2015 issuance which provided clarification on the exceptions to the examination frequency for banks and trust companies; included the Continuous Examination Program definition in the Scope of Examinations section; expanded the IT Examination Scope and Frequency Schedule for Banks to include bank asset size, and updated the Department contact information for the Chief IT Security Examiner provided at the end of the policy.

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 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 Chief IT Security Examiner. The Department utilizes four types of examination scopes for IT reviews: Level I Full Scope, Level II Full Scope, Visitation, and Continuous.

- A Level I Full Scope Examination (Level I) is the most comprehensive with the Department’s IT specialists completing procedures that are designed to assess the entity’s IT risks and controls. An overall rating will be issued and included in a Report of Examination produced for the entity.
- A Level II Full Scope Examination (Level II) allows IT specialists to focus on the highest risk areas of the entity, while excluding certain assignments determined to be of lower risk. IT Specialists will continue to review all critical aspects of the IT operations to the extent needed to assign an overall rating. An overall 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 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 Level I and Level II examinations as well as the CEP 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 Chief IT Security Examiner in collaboration with the applicable Regional Director or Chief Trust Examiner. These reviews and scope determinations will be performed under the direction of the Chief IT Security Examiner 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 bank or trust company or delivered under separate cover as an independent Report of Examination or Letter of Findings as determined by the Chief IT Security Examiner and applicable Regional Director or Chief Trust Examiner.

EXAMINATION FREQUENCY***State-Chartered Banks***

The frequency of an IT examination generally follows the frequency of safety and soundness examinations for state-chartered banks, with the IT examination due within 120 days prior to the due date of the safety and soundness examination. 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.

The following chart details the *general* criteria for determining the IT examination frequency for state-chartered banks.

IT EXAMINATION SCOPE AND FREQUENCY SCHEDULE FOR BANKS

BANK ASSET SIZE	BANK COMPOSITE AND CAPITAL CRITERIA	BANK EXAMINATION FREQUENCY	IT EXAMINATION RATING	IT EXAMINATION SCOPE AND FREQUENCY
\$10 Billion or Greater ¹	1 or 2 Composite	Continuous Examination Program. A composite risk rating is assigned every 12 months.	1 or 2	12 months; Continuous Examination Program. A composite risk rating is assigned every 12 months.
\$10 Billion or Greater ¹	3, 4, or 5 Composite	Continuous Examination Program. A composite risk rating is assigned every six months.	3, 4, or 5	Continuous Examination Program. A composite risk rating is assigned every 6 months. Additional monitoring of targeted areas in the interim.
Greater Than \$1 Billion But Less Than \$10 Billion	1 or 2 Composite	12 months.	1 or 2	Level I or Level II every 12 months.
Greater Than \$1 Billion But Less Than \$10 Billion	1 or 2 Composite	12 months.	3, 4, or 5	Level I every 12 months; Mid-point in the examination cycle, perform a Level I examination, Visitation or Off-site review.

BANK ASSET SIZE	BANK COMPOSITE AND CAPITAL CRITERIA	BANK EXAMINATION FREQUENCY	IT EXAMINATION RATING	IT EXAMINATION SCOPE AND FREQUENCY
\$1 Billion or Less	"Well capitalized" as defined by 12 C.F.R. 325.103 (b)(1) (member bank) or §325.103(b)(1) (nonmember bank) AND 1 or 2 Composite Rating with 1 or 2-Rated Management	18 months.	1 or 2	Level I or Level II every 18 months.
\$1 Billion or Less	"Well capitalized" as defined by 12 C.F.R. 325.103 (b)(1) (member bank) or §325.103(b)(1) (nonmember bank) AND 1 or 2 Composite Rating with 1 or 2-Rated Management	18 months.	3, 4, or 5	Level I every 18 months; Mid-point in the examination cycle, perform a Level I examination, Visitation or Off-site review.
\$1 Billion or Less	1 or 2 Composite With Management Rating >2 OR Not "well capitalized" as defined by 12 C.F.R. 325.103(b)(2) and 1 or 2 Composite	12 months.	1 or 2	Level I or Level II every 12 months.

BANK ASSET SIZE	BANK COMPOSITE AND CAPITAL CRITERIA	BANK EXAMINATION FREQUENCY	IT EXAMINATION RATING	IT EXAMINATION SCOPE AND FREQUENCY
\$1 Billion or Less	1 or 2 Composite With Management Rating >2 OR Not "well capitalized" as defined by 12 C.F.R. 325.103(b)(2) and 1 or 2 Composite	12 months.	3, 4, or 5	Level I every 12 months; Mid-point in the examination cycle, perform a Level I examination, Visitation or Off-site review.
Any Size	De Novo and 1 or 2 Composite	Visitation within first six months of opening. Level I examination 12 months after opening and annually thereafter for the first five years of operation. Commissioner may alter this schedule to align with the applicable federal regulatory agency or division policy.	De Novo and 1 or 2	Visitation within first 6 months of opening. Level I or Level II Examination 12 months after opening and annually thereafter for the first five years of operation. Commissioner may alter this schedule to align with the applicable federal regulatory agency or division policy.
Less than \$10 Billion	3, 4 or 5 Composite	Level I examination every 12 Months. FDIC Visitation or Interim Risk Examination and Assessment (IREAP) to be performed approximately six months after the Level I examination.	1 or 2	Level I or Level II every 12 months. IT exam not required with the bank IREAP

BANK ASSET SIZE	BANK COMPOSITE AND CAPITAL CRITERIA	BANK EXAMINATION FREQUENCY	IT EXAMINATION RATING	IT EXAMINATION SCOPE AND FREQUENCY
Less than \$10 Billion	3, 4 or 5 Composite	Level I examination every 12 Months. FDIC Visitation or Interim Risk Examination and Assessment (IREAP) to be performed approximately six months after the Level I examination.	3, 4, or 5	Level I every 12 months; Mid-point in the examination cycle, perform a Level I examination, Visitation or Off-site review. IT exam not required with the bank IREAP

- (1) The Commissioner or Deputy Commissioner may designate any institution with total assets over \$5 billion to be examined under the CEP.

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 Level I 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 Chief IT Security Examiner based on factors such as severity of weaknesses, management's capability, and information in progress reports. A composite IT rating will be assigned at a Level I examination and a Report of Examination will be provided to the bank. If a visitation 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

Change in Scope of Safety and Soundness Examination:

If the safety and soundness IREAP 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:

- If the IT Rating is a 1 or 2:
 - A Level I or II Full Scope IT exam will be performed approximately 6 months after the converted Full Scope exam. The IT examination frequency will then follow the 18 month cycle; or
- If the IT Rating is a 3, 4, or 5:
 - A Level I Full Scope IT examination will be performed approximately 6 months after the converted examination followed by a Level I examination,

Visitation, or Off-site review in 12 months. The IT examination frequency will then follow the 18 month cycle.

Change in Safety and Soundness Examination Frequency

- 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 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 the due date for the trust company examination. 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.

The following chart details the *general* criteria for determining the IT examination frequency of state-chartered trust companies.

IT EXAMINATION SCOPE AND FREQUENCY SCHEDULE FOR TRUST COMPANIES

TRUST COMPANY COMPOSITE RATING AND CRITERIA	TRUST COMPANY FREQUENCY	IT Examination Rating	IT Examination Scope and Frequency
1 or 2 CAMEL or 1 or 2 UITRS	18 Months	1 or 2	Level I or Level II every 18 Months.
		3, 4, or 5	Level I every 18 months; Mid-point in the examination cycle, perform a Level I, Visitation examination, or Off-site review.
3, 4 or 5 CAMEL or 3, 4 or 5 UITRS -OR- 3-Rated Management and 1 or 2 CAMEL or 1 or 2 UITRS	12 Months	1 or 2	Level I or Level II every 12 months.
		3, 4, or 5	Level I every 12 months; Mid-point in the examination cycle, perform a Level I, Visitation examination or Off-site review.
New Trust Company - Not Yet Rated	Initial exam in six to 12 months, then every 12 months for three years.	1, 2, 3, 4, or 5	Level I or II within six to 12 months and annually thereafter. May perform Level I or visitation in interim during first five years.

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 Level I 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 Chief IT Security Examiner based on factors such as severity of weaknesses, management's capability, and information in progress reports. A composite IT rating will be assigned at a Level I examination and a Report of Examination will be provided to the trust company. If a Visitation 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**Change in Safety and Soundness Examination Frequency**

- 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 Chief IT Security Examiner. 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 banks, and if they are subject to examination by other regulatory agencies.

Only Tier 1 TSPs are subject to routine IT examinations by the Department. Tier 2 and Tier 3 TSPs are not subject to routine examination by the Department and are generally either part of the FFIEC Multi-Regional Data Processing Servicers (MDPS) program or provide only ancillary (non-critical) data processing service.

The three tiers are defined as follows:

Tier 1

These TSPs are generally owned, controlled, or otherwise affiliated with a bank that provides processing 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 Chief IT Security Examiner 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 Level I or visitation examination may be performed. The scope and timing of the interim examination will be determined by the Chief IT Security Examiner 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 that are included in the FFIEC's Multi-Regional Data Processing Servicers (MDPS) Program, such as large national data processing companies. 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 generally provide only ancillary (non-critical) technology services and/or provide services to only a small number of state-chartered banks. Tier 3 TSPs are generally located out of state and are not subject to routine examinations by the Department. Tier 3 TSPs are subject to examinations on a case by case basis. The Department monitors examination data on Tier 3 TSPs received from the FFIEC member agencies.

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 the Department's Chief IT Security Examiner, Linda Pearson, at 210-271-3923.