TEXAS DEPARTMENT OF BANKING
INFORMATION TECHNOLOGY EXAMINATION
REQUEST LIST - CHARTER INVESTIGATION

The following is a list of documents that will be used in the offsite IT review for your charter application. Examiners will need an electronic ***copy*** of a requested item.

Please submit the electronic documents, including this list with contacts identified, using a secure, encrypted method of transmission. We recommend that files be saved in a folder then zipped to compress the file size and uploaded.

	REQUESTED ITEMS - IT CHARTER INVESTIGATION	CONTACT PERSON (Name and Number)
1.	Provide a copy of the current and/or proposed information technology (IT) organizational chart.	
2.	Provide the names, titles, job descriptions, and biographies of the IT security officer, system administrator, and business continuity planning coordinator. If these duties will be outsourced, provide the name and address of the firm and a brief description of the services to be provided. Provide a copy of the contract(s) if available.	
3.	Outline the current and/or proposed internal and external IT audit program and audit scope.	
4.	Provide the name, title, job description, and biography of the IT auditor, both internal and external, if applicable. If these duties will be outsourced, provide the name and address of the firm if already selected. Provide a copy of the engagement letter if available.	
5.	Identify the anticipated date and frequency that the IT audit/independent reviews will be performed.	
6.	Describe plans for performing penetration tests and vulnerability assessments. Provide the name and address of the firm(s) that will be completing these services if already selected.	
7.	Provide a copy of the most recent IT audit report, network penetration test, and network vulnerability assessment if applicable.	

	REQUESTED ITEMS - IT CHARTER INVESTIGATION	CONTACT PERSON (Name and Number)
8.	Provide a copy of the network topology/diagram (IP addresses are not necessary).	
9.	Describe all critical IT platforms. Include a list of all hardware and software currently in use and indicate whether the software was purchased or developed in house. Also include a list of all hardware and software that will be added within the next 12 months along with any additional start-up costs that will be needed for hardware, software, or personnel. Complete the attached Products and Services Template.	
10.	Complete the Information Technology Profile (ITP) Questionnaire. (This will be provided to you separately)	
11.	Provide a copy of the most recent cybersecurity risk and maturity (preparedness) assessments, if available.	
12.	List all current and/or proposed Internet website addresses. Indicate whether the site is or will be hosted internally or externally. If externally hosted, indicate the name and location of the website service provider if available. Also indicate whether or not the website is or will be transactional.	
13.	Provide a copy of the Business Continuity/Disaster Recovery plans (including the business impact analysis and risk assessment used to develop the plan).	
14.	Provide a description of the current and/or planned backup procedures for all critical systems.	
15.	Provide a description of current and/or planned strategies for testing the disaster recovery/business continuity plans.	
16.	Identify the location of any current and/or planned disaster recovery sites and off-site storage locations.	
17.	Provide a copy of the most recent disaster recovery test results.	
18.	Identify the location of any current and/or planned disaster recovery sites and off-site storage locations.	

	REQUESTED ITEMS - IT CHARTER INVESTIGATION	CONTACT PERSON (Name and Number)
19.	**Policies and Procedures** Please provide a copy of all applicable IT-related policies, procedures, and standards including but not limited to: • Operational Policies and Procedures • IT Strategic Plan • IT Audit Policy • Information Security Program that conforms with the Gramm-Leach-Bliley Act (include a copy of the most recent report to the Board on the overall status of the program) • Risk Assessment performed in conjunction with the Gramm-Leach-Bliley Act Information Security Program • Incident Response Program • Vendor Management Program • Funds Transfer Program • Account Takeover Program • Identity Theft Red Flags Program	