BOK Financial Information Packet

NOT FOR USE IN CONNECTION WITH THE SALE OR PURCHASE OF SECURITIES

1 COMPANY INFORMATION

Contact information	BOKF, NA P.O. Box 2300 Tulsa, OK 74192 BOKF, NA's ("BOKF" or the "Bank") corporate headquarters is located at Bank of Oklahoma Tower, Boston Avenue at Second Street, Tulsa, Oklahoma 74172.
Description	BOKF is a regional financial services company offering a broad range of financial products and services, including commercial lending, cash management, mortgage banking, merchant and debit card processing, fiduciary services, risk management and brokerage and trading services to middle-market and small businesses, financial institutions and consumers. BOKF strives to provide nationally competitive products with personalized, responsive client service. BOKF assets exceed $40 billion. The Bank operates primarily in the metropolitan areas of Tulsa and Oklahoma City, Oklahoma; Dallas, Fort Worth and Houston, Texas; Albuquerque, New Mexico; Denver, Colorado; Phoenix, Arizona, and Kansas City, Kansas/Missouri.
History	BOKF traces its roots to 1910, when Harry Sinclair and other noted Tulsa oilmen founded Exchange National Bank of Tulsa to grant loans for their new oil fields. In the decades that followed, the Bank achieved numerous important milestones. By 1925, the Bank was 90 times its original size in terms of assets. It survived the Wall Street panic of 1929 without losing a single dollar. After WWII, the Bank made the first GI loan in Tulsa. The Bank was instrumental in changing arcane laws that made it difficult to install ATMs when they became popular. In 1975, the Bank expanded to Oklahoma City and changed its name to Bank of Oklahoma. In 1991, BOK Financial Corporation ("BOK Financial") was formed and the growth continued. Today, the Bank is a multi-billion dollar regional financial services organization. It operates in eight states and provides commercial and consumer banking, mortgage, wealth management and electronic funds transfer services nationwide.[i]
Strategic Objective	BOKF's objective is to build a recession-proof bank that will outperform peer banks across the economic cycle. This is accomplished through a primary focus on organic growth, disciplined credit underwriting, investment in fee-generating businesses, and disciplined stewardship of capital. The Bank operates primarily in the metropolitan areas of Tulsa and Oklahoma City, Oklahoma; Dallas, Fort Worth and Houston, Texas; Albuquerque, New Mexico; Denver, Colorado; Phoenix, Arizona, and Kansas City, Kansas/Missouri. BOKF supplements organic growth through opportunistic acquisitions

	and investments in new entrepreneurial businesses, by hiring talent to enhance competitiveness, adding locations and broadening product offerings. The Bank's operating philosophy embraces local decision-making in each of its geographic markets while adhering to common Company standards. [ii] One of BOKF's notable strengths is its diverse revenue streams. Noninterest revenue represents approximately 45% of total revenue.
Structure	BOK Financial is a financial holding company incorporated in the state of Oklahoma in 1990. Its activities are governed by the Bank Holding Company Act of 1956 ("BHCA"), as amended by the Financial Services Modernization Act also known as the Gramm-Leach-Bliley Act and the Dodd-Frank Wall Street Reform and Consumer Financial Protection Act (the "Dodd-Frank Act"). BOKF, NA, a national bank, is a wholly owned subsidiary bank of BOK Financial. BOKF, NA operates TransFund, Cavanal Hill Investment Management, BOK Financial Asset Management, Inc. and seven full service banking brands: Bank of Albuquerque, Bank of Oklahoma, Bank of Texas, and BOK Financial for Arizona, Arkansas, Colorado, and Missouri. On December 1, 2016, BOK Financial acquired Missouri Bank and Trust Company Kansas City d/b/a Mobank as a wholly owned subsidiary bank of BOK Financial, more than doubling the market share in the Kansas City area. Mobank was merged into BOKF, NA on February 17, 2017. The Bank of Kansas City banking centers were converted to the Mobank brand. Mobank (including Mobank Mortgage and Mobank Private Wealth) and Bank of Arkansas were rebranded BOK Financial on October 29, 2019. On October 1, 2018, BOK Financial acquired CoBiz Financial as a wholly owned subsidiary, greatly enhancing market presence in the Colorado and Arizona markets. CoBiz 's banking subsidiary was merged into BOKF, NA in the first quarter of 2019. Other wholly owned subsidiaries of BOK Financial include BOK Financial Securities, Inc., a broker/dealer engaging in retail and institutional securities sales and municipal bond underwriting and The Milestone Group, Inc., an investment adviser to high net worth clients. [iii]
License	BOKF, NA, a national bank, is a wholly owned subsidiary bank of BOK Financial Corporation, formed under the federal laws of the United States. BOKF, NA is regulated by the Office of the Comptroller of the Currency and the FDIC. As a national bank, BOKF, NA is not required to be licensed by any state regulatory body and is instead regulated by the federal government.

Current number of employees and locations	As of December 30, 2019, the subsidiaries of BOK Financial employed a total of 5,141 full-time equivalent employees.
Products and services	BOKF's primary focus is to provide a comprehensive range of nationally competitive financial products and services in a personalized and responsive manner. Products and services include loans and deposits, cash management services, fiduciary services, mortgage banking, and brokerage and trading services to middle-market businesses, financial institutions and consumers. Commercial banking represents a significant part of the Bank's business. BOKF's credit culture emphasizes building relationships by making high quality loans and providing a full range of financial products and services to our customers. BOKF's energy financing expertise enables the Bank to offer commodity derivatives for customers to use in their risk management. The Bank also offers derivative products for customers to use in managing their interest rate and foreign exchange risk. The bank further offers merchant and debit card processing.
Biographies of key professionals	Refer to link https://investor.bokf.com/Officers-and-Directors
Market share	For Q4 of 2019, BOK Financial reported total consolidated assets in excess of $40 billion and is ranked as a top 25 U.S.-based bank. Refer to link http://investor.bokf.com/SEC-Filings
Employment Practices	The subsidiaries of BOK Financial are committed to a work environment in which individuals are treated with respect and dignity. BOKF expects a professional atmosphere that promotes equal employment opportunities to applicants and employees without regard to race, religion, color, gender, sexual orientation, age, national origin, disability, military or veteran status, genetic information, or other criteria protected by federal, state or local law and is free from prohibited discriminatory practices, including all types of unlawful harassment. The subsidiaries of BOK Financial have policies and procedures in place to meet these expectations.
Diversity Commitment	BOKF celebrates differences through inclusion, by valuing a diverse workforce, and making an effort to include different employee perspectives.[iv] A mosaic of differences among employees in areas such as education, age, gender, religion, race, culture, ethnicity, and other unique characteristics and experiences makes the Bank stronger.

2 FINANCIALS

Total assets	BOK Financial's quarterly and annual U.S. Securities and Exchange Commission ("SEC") filings are available on the web: BOK Financial Corporation – Financial Information – SEC Filings
Statement of financial condition	Financial statements for BOK Financial can be found at: BOK Financial Corporation – Financial Information – SEC Filings
Credit Ratings	Credit ratings for BOK Financial can be found at: http://investor.bokf.com/creditratings.aspx?iid=100003
Audited Financial Statements	BOKF, NA, a wholly owned subsidiary of BOK Financial Corporation (see Company Information section in the BOKF Information Packet provided), does not have separately audited financials, although it does file separately with the Office of the Comptroller of the Currency and the FDIC, quarterly financial information in the form of call reports. BOKF, NA's financials are consolidated with its parent corporation, BOK Financial Corporation, a NASDAQ publicly traded company, whose combined financials (which consist primarily of BOKF, NA) are audited by Ernst & Young and filed with the Securities Exchange Commission and may also be found on the BOK Financial Corporation investor page.

3 COMPLIANCE AND REGULATORY

Compliance Officer	Jo Ann Stall, Chief Compliance Officer
Compliance policies and procedures	Policy, procedure and practice reviews are conducted routinely and when warranted by changes to applicable laws or the issuance of applicable regulatory guidance.

Compliance Program	The Chief Compliance Officer, in a collective effort with Compliance staff, the Lines of Business (LOB), the Office of General Counsel, and the Compliance Committee, is responsible for overseeing the Compliance Management Program. The Bank's Compliance Management Program includes the following components: • Risk Identification and Assessment • Policies and Procedures • Monitoring and Testing • Complaint Management • Training • Issue Escalation • Corrective Action • Accountability • Reporting • Advising[v]
Regulatory environment	BOK Financial subsidiaries are regulated by several regulatory bodies including: the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Consumer Financial Protection Bureau (CFPB), U.S. Securities and Exchange Commission (SEC), and Financial Industry Regulatory Authority (FINRA).
Bank Secrecy Act (BSA) and Anti-money Laundering (AML)	BOK Financial and BOKF are committed to compliance with the requirements of the Bank Secrecy Act ("BSA"), USA PATRIOT Act ("USAPA"), Office of Foreign Assets Control ("OFAC"), and related Anti-money Laundering ("AML") regulations through its BSA/AML Program. The BSA/AML Program includes the designation of a BSA Officer, the implementation of internal controls, and independent testing and training programs commensurate with BOKF's size and risk profile. Further, the BSA/AML Program implements procedures for a Customer Identification Program ("CIP"), BSA risk assessment, monitoring and reporting suspicious activity, performing customer and enhanced due diligence, currency transaction reporting, monetary instrument recordkeeping, OFAC monitoring, record retention, training, and various other requirements of the regulations.

Public and non-public information	The protection of Non-Public Personal Information ("NPPI") is of paramount importance. The Gramm-Leach-Bliley Act of 1999 ("GLBA") establishes standards for financial institutions relating to administrative, technical, and physical safeguards for customer records and information. The purpose of these safeguards is to ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. BOKF has policies, procedures, and processes in place designed to safeguard customer records and information, including: • Information Security Program Policy & Standards (ISPP) • Data Loss Prevention Policies, procedures and practices • BOKF Identity Theft Program and Policy. Training related to safeguarding customer information is provided to all applicable employees. Additionally, BOKF employees sign and attest annually that they will not disclose or use any confidential or secret information about the employer or any of the employer's affiliates or clients except as necessary in the conduct of the employer's business or unless authorized in writing by the employer.
Procedures for safeguarding and preservation of records containing Protected Health Information, Personally Identifiable Information or other information subject to data protection and privacy laws (e.g., HIPAA, GLBA, COPPA) and contracts	BOKF's privacy and data protection program includes, but is not limited to, establishing data privacy guidelines, managing the Identity Theft Program and Data Loss Prevention Programs, conducting annual and periodic privacy training and awareness courses. Awareness campaigns include newsletters and articles, as well as desk tents and printed materials. Computer systems that contain sensitive customer data are stored in a secure, climate controlled data center with no direct access from outside doors or windows. Building access controls include security guards, magnetic door locks and CCTV.
Protection of our clients against financial loss due to fraudulent acts	BOKF maintains a tested and documented internal control structure that safeguards customer assets. Supplementing this, BOKF maintains insurance coverage that includes financial crimes and employee fraud protection. Refer to Insurance coverage.

Describe the formal process for interpreting, implementing and testing regulatory and legal changes timely	Corporate Compliance Management and the Office of the General Counsel regularly monitor federal regulatory changes applicable to the Bank. When necessary, policies, procedures and/or processes are created or modified in order to comply with new regulatory requirements. Depending on the nature of a regulatory change, the Compliance testing team and/or Audit will conduct post implementation testing.

4 LEGAL

Litigation (including arbitrations, formal investigations and disciplinary actions by any regulatory organizations in the last 12 months)	As a national banking association, BOKF is subject to multiple regulatory examinations on a regularly recurring basis. These examinations result in suggestions for improvement, identify matters requiring special attention, and specify corrective actions, from time to time. In the ordinary course of business, BOK Financial and its subsidiaries are subject to legal actions and complaints from time to time. Management believes, based upon the opinion of counsel, that the foregoing actions and liability, if any, resulting from the final outcomes of the foregoing proceedings, will not have a material effect on BOK Financial's financial condition, results of operations or cash flows.
Insurance coverage	BOKF's insurance philosophy is to manage risk where we can affordably do so and transfer risk that is catastrophic or unmanageable. All coverage is continually renewed prior to expiration dates.

5 RISK MANAGEMENT

Risk management process	Credit Risk and Enterprise Risk are independent functions. The Chief Credit Officer oversees the credit risk function and reports to the Chief Executive Officer. The Chief Risk Officer oversees the remaining risk disciplines and reports to the Chief Executive Officer and the Risk Committee of the Board of Directors. An Enterprise Risk Management (ERM) Framework and Risk Assessment Methodology exist and are used for assessing risk exposures across the various risk categories identified in the ERM Framework.
Risk management and oversight responsibilities	The Board and its committees form the basis for risk oversight and approve the risk appetite of the company. Executive management is charged with translating the risk appetite into appropriate limits and establishing an effective risk culture. The independent Risk

	Management group forms the second line of defense, which provides oversight of business risk identification, monitoring and testing as well as escalation of issues as appropriate.

6 INFORMATION SECURITY MANAGEMENT

Qualified individual or group responsible for information security	BOKF has a Chief Information Security Officer who oversees dedicated staff responsible for the following services: Security Risk Management, Business Continuity, Data Protection, Identity and Access Management, Security Operations, Security Incident Management, Security Awareness, Threat Management, and Security Architecture and Engineering.
Formal information classification procedure	Information classification levels are Public, Confidential, and Restricted Confidential.
Formal acceptable use rules established for assets	Acceptable use policies are included in the employee Standards of Conduct. The Information Security Program includes a formal set of policies and standards that are updated based on changes to the Information Security threat landscape and are approved by executive leadership.
All personnel with access to client, confidential or proprietary information are required to sign confidentiality agreements	BOKF requires that employees certify annually that they adhere to and comply with the Standards of Conduct. As part of fulfilling the requirements of the Standards of Conduct, all employees are required to comply with all policies and procedures of the Bank and all laws and regulations applicable to the Bank's business activities or applicable to the employee individually. BOKF directors, officers, and employees must protect confidential or proprietary information at all times.
Background checks and screening requirements for applicable positions	• Social Security Number Verification • Education Verification • Employment Verification • Criminal Background Check • Drug Screening In accordance with applicable law, it is the policy of the Bank to fingerprint all post-offer, pre-employment, newly hired or rehired associates or those transferees to BOKF entities and their affiliates that are regulated by the Federal Deposit Insurance Act and/or the Securities Exchange Act of 1934.
Security training and awareness program	Employees are given information security training during the new-hire orientation process. Computer Based Training (CBT) courses and testing are assigned yearly. Targeted risk and control training is

	given both in person and through CBTs annually. Social Engineering tests are conducted periodically throughout the year through simulated Phishing campaigns.
Disciplinary procedures for security violation	BOKF addresses performance and conduct issues as necessary. The type of corrective action administered, up to and including termination, depends upon the severity or frequency of the problem involved.
Return of assets upon termination	Employees, contractors and third-party users are required to return all organization-owned assets and/or data in their possession upon termination of their employment, contract or agreement.
Removal of access rights or permissions when associate is terminated or resigns	Access is disabled according to the last day worked of the associate as input into the HR system. Network access to BOKF is automatically disabled within 24 hours. Access to critical applications deemed high value assets is disabled within 3 business days. All other access is disabled within 10 business days.
Application and support development procedures	During the development phase of the Software Development Lifecycle (SDLC), developers perform secure static code scanning as well as code quality scanning. Static code reviews are performed using the HP Fortify tool that identifies potential security concerns. Sonar is used for continuous inspection of code quality (e.g. duplicated code, coding standards, etc.) for digital banking related projects. This type of scanning is performed throughout the code lifecycle.
Segregation of information security administration duties and responsibilities	Segregation of duties exists between individuals approving access changes and individuals administering changes. Segregation of duties exists between individuals administering access changes and individuals performing business transactions within the application.
Procedures for usage and management of all types of removable media	Policies and procedures are in place to prevent the use of Universal Serial Bus (USB) mass storage devices. USB usage is controlled through Data Loss Prevention (DLP) policies that block the movement of sensitive customer data. For business processes that require the movement of sensitive data on removable storage devices, encryption is used to protect the information on USB devices. Backup media is encrypted before movement to offsite storage.
Procedures for maintenance and destruction of media including paper documents containing sensitive information	BOKF has procedures for maintenance and destruction of media, including paper. Physical documents are handled through on-site mobile destruction services provided by a third party. Hardware disposal requires a Department of Defense (DOD) approved disk wipe, or physical destruction of drives.

Procedures for handling and storage of information to protect it from unauthorized disclosure or misuse	Computer systems that contain sensitive customer data are stored in a secure, climate controlled data center with no direct access from outside doors or windows. Building access controls include security guards, magnetic door locks and closed circuit television (CCTV).
Secure e-mail system for internal and external use and procedures followed when sending sensitive data to an external party	BOKF has a secure e-mail system for internal and external use. Sensitive e-mails to external parties are encrypted. Data Loss Prevention tools monitor and block the movement of sensitive customer information both at the endpoint and through network protocols.
Log information, system logging facilities, system administrator and system operator activities are logged and protected	Logs are stored during active retention periods in a secure location with restricted access.
Retention period for logs and analysis of all system operation fails and data security breaches	Logged data sets that are classified as business records are archived for a time duration that has been determined by BOKF records management, in consultation with Legal and Compliance staff.
Account administration for operating system, user accounts and service application	BOKF employees and contingent workers are provided unique identifiers for authentication purposes. The creation of non-human identities is requested via an enterprise request tool. Privileged non-human IT accounts are managed by a privileged access management tool.
Data Backup	Application and system backups are conducted through a combination of block-level storage replication and agent based point in time backups.
Prevent leakage of confidential or sensitive information in any form	A layered defense-in-depth approach is used in the information security architecture. Endpoints are managed with multi-functioning agents for malware, network anomalies and data loss protection. Firewalls are deployed at trust boundaries. Network Intrusion Detection System/Intrusion Prevention System (IDS/IPS) are positioned at ingress and egress points. Web Application Firewalls are deployed for all customer facing online banking applications.
Reporting security weaknesses	Self-Identified security control deficiencies are centrally tracked by the Enterprise Risk Management team.

Reporting and escalation process for handling security incidents (logged, monitored, reviewed, reported, investigated and followed up)	A computer Incident Response Plan has been developed to outline the tasks and activities, roles and responsibilities, and escalation procedures for security incidents. Chain of custody processes are followed when documents are requested by legal.
Learning from information security incidents	After Action Reports (AAR) provide all of the details that accurately describe the aspects of the incident. These details should include: • When an event was reported • Any correlated alerts or events • Technologies and business processes affected • Personnel and vendors involved • Triage analysis performed • When the Incident Response Lead declared the event an incident • Steps taken for containment • Overall outcome This report will also identify the lessons learned, process successes and challenges, technical limitations, and root cause analysis. The AAR template may be found in the Communications Plan.
Electronic file transmissions secured and supported	Secure Shell (SSH) keys for secure file transmissions are centrally housed in an application managed by Transmission services.
Reviews security logs and audit reports	Security logs are centrally managed with a Security Information and Event Management (SIEM). A Security Operation Center (SOC) is staffed with security analysts 24x7x365 to respond to critical incidents generated by the SIEM.

7 NETWORK SECURITY MANAGEMENT

Network Configuration	Systems and applications are segmented using a multi-tier architecture (N-Tier) design strategy. The N-Tier design architecture includes a Web DMZ, Application DMZ, Vendor DMZ, and internal network segmentation by region and location.
Approach for protecting network devices	A layered network security architecture is employed to protect network devices throughout the environment. Systems and devices are managed through a lifecycle approach that includes hardened security baseline configurations, change management, network vulnerability scanning and testing. Wireless networks are logically segregated from all internal network segments.

Vulnerability scans on information technology systems, networks and supporting security systems	The vulnerability management program includes scheduled system scans on a continuous basis. Application security assessments are performed on all customer facing online banking platforms. Yearly external penetration testing is conducted by a third party.
Audit logs are kept to assist in future investigations and access control monitoring	Security device logs are sent to the SIEM for correlation and analysis.
Systematic review of user access rights at regular intervals	Entitlement reviews are conducted by the Identity and Access Management group with frequencies dictated by the criticality of the application or system. Entitlement review processes are audited by the internal audit function.
User authentication for remote access	Multi-factor authentication is used to authenticate remote users accessing the corporate network through the VPN.
Wireless network devices	Wireless access networks are segmented from the corporate network, and utilize industry standard encryption.
Intrusion Detection and Prevention	Network IDS/IPS are positioned at ingress and egress points.
Server and network system clocks	Server and network system clocks are synced with designated internal and external time servers.
User identification and authentication	Access to BOKF systems require a user ID and a password that is compliant with the Access Management Standard. Access is requested via an enterprise request tool and approved by the user's manager, as a minimum.
Sharing user IDs or passwords	BOKF prohibits sharing user IDs or passwords.
Password management policy	The password policy includes: • Password requirements include: o Minimum Character Length ▪ Passwords must be a minimum of eight (8) characters, with sixteen (16) recommended for privileged accounts. o Password Complexity ▪ Passwords must consist of three (3) out of four (4) possible character sets o Password Expiration

	▪ Change password every 90 days (max) for business user accounts and every 45 days (max) for accounts that are considered privileged. o Password History Policy ▪ History requirements must be set to remember, at a minimum, the last four (4) passwords and limit reuse o Account Lockout ▪ Accounts must be locked or disabled after five (5) or fewer failed log-on attempts.
Mobile computing and communications	BOKF allows mobile devices that are both corporate owned and personally owned to connect in a secure environment. Mobile devices are managed by a Mobile Device Management (MDM) tool.
Data stored on the mobile device	Sensitive data stored on mobile devices is required to be encrypted and other safeguards are deployed to protect stored data from unauthorized access or misuse. Mobile devices managed by MDM require authentication (PIN) and provide device partitioning and encryption.
Access control to program source code	Access to source code is restricted to those with a specific business need.
Precautions taken against cross-site scripting and SQL injection attacks, parameter tampering, etc.	BOKF employs multiple coding techniques, penetration testing by outside professionals and regression testing to ensure timely identification and remediation of code vulnerabilities.
Documented procedures for remediating known vulnerabilities	BOKF has a formal technical vulnerability management program that includes the identification and remediation of vulnerabilities. Vulnerability scans and health checks of these devices are conducted on a regular basis.
Change management procedures for implementing changes to all hardware, software, etc.	Prior to implementation, all proposed changes must be aligned to a specific requirement, be tested, and approved by senior management. A workflow or issue-tracking tool is used to ensure the proper phases have been completed, all necessary artifacts exist, and the required approvals have been documented.
Problem management procedures	The problem management process is formal and documented and makes use of an IT Service Management (ITSM) tool.

Protection of permitted third-party connections to the network or data center	Third parties are monitored through a Security Scorecard service for external indicators of information security weakness. VPN logs are stored within the SIEM application. Data transfers are centralized within the Transmission Services area and include provisions for encryption of data both at rest and in transit. Secure protocols (Hypertext Transfer Protocol Secure (HTTPS), are used for file transfers and loads to and from customers and business partners.
Controls and protection for servers and workstations against malicious codes	Malware and malicious code detection occurs at the Simple Mail Practical (SMTP) gateways, web proxy devices and at endpoints (through agent based heuristics and scanning). Endpoint agents are centrally managed and signatures are deployed when made available by the vendor. Compliance checks are run through endpoint agent analysis.

8 RESILIENCE

Program Governance	BOKF is committed to providing its stakeholders with a risk-based enterprise-wide Business Continuity Management Program ("BCMP"). BCMP is a key component of BOKF's corporate governance and Enterprise Risk Management. The BCMP is designed to ensure the operational viability of the Bank is maintained in the event of an outage or interruption to mission-critical/essential business operations. The BCMP Policy for BOKF is sponsored and endorsed by the executive leadership. Oversight of the BCMP is performed by the Board of Directors, which has been delegated to the Risk Committee of the Board. The BCMP Policy, Standards and Procedures are derived from the FFIEC IT Examination Handbook of Business Continuity Planning and the ISO 22301 international business continuity management standard, with the ISO 22301 mapped to the Disaster Recovery Institute International ("DRII") Business Continuity Professional Practices.
Business Impact Analysis	BOKF maintains and documents an enterprise-wide BIA to assess and prioritize business functions and processes. Business functions and processes are evaluated to determine interdependencies between critical operations, departments, personnel and services, as well as the impact of interruptions to business operations, legal and regulatory obligations, and reputational, financial, and client experience considerations. Results of the analysis are utilized to establish Recovery Time Objectives (RTO) and Recovery Point Objectives

	(RPO) for the purpose of establishing the critical path for recovering business functions and processes.
Risk Assessments	BOKF maintains and documents Risk Assessments to identify and analyze realistic threat scenarios that could potentially disrupt the ability to do business. Risk Assessments evaluate the effectiveness of existing controls (of the facilities in which it operates) and the policies and procedures implemented to recover, resume and maintain normal business operations (of the third party providers with which it does business), in response to natural, technical and manmade events().
Business Continuity Strategies	BOKF utilizes information collected during the BIA and Risk Assessments to identify and define acceptable recovery strategies for the organization. Acceptable recovery strategies support the RTO and RPO objectives for business operations and technology identified in the BIA. BOKF has strategies that support alternate recovery sites, transference of operations and remote recovery of critical business operations and technology.
Incident Response	BOKF maintains enterprise-wide incident response plans to protect life, property and the environment. Response capabilities include an incident management system to provide command, control and coordination of resources during an event.
Plan Development and Implementation	BOKF maintains Business and Disaster Recovery Plans incorporating the BIA and Risk Assessments to document short-term and long-term strategies to recover, resume and maintain critical business operations and technology. The recovery plans address non-specific continuity threats including, but not limited to, Loss of Facility, Loss of Systems, Loss of People, Loss of Vendor, Loss of Data and Multi-Loss Scenarios. Plans are reviewed at least annually or as material changes are made in the production environment.
Awareness and Training	BOKF maintains an enterprise-wide business continuity training and awareness program that includes training for management, recovery team members and stakeholders.
Plan Exercises, Assessment and Maintenance	BOKF maintains an enterprise-wide testing program to ensure the recovery plans remain viable. The BIA and Risk assessments serve as the foundation for the comprehensive and integrated testing program. Frequency and complexity of exercises are commensurate with the criticality of business functions and technology. Revisions to the recovery plans and testing program are based on changes in business operations, audit and examination recommendations and test results. Testing standards include requirements for reporting and

	remediation for noncompliance. Key tests are observed, verified and evaluated by independent parties, such as internal audit and external regulators.
Disaster Recovery	BOKF maintains a disaster recovery program with a backup data center for critical applications and data.

9 THIRD PARTY PROVIDERS

BOKF's third party management program.	BOKF's vendor management program is a two tiered approach. The business line is the first line of defense and is supported by the Corporate Vendor Management Office. The business line is responsible for managing the risk of each vendor relationship it engages. This tier involves planning the third party engagement, performing risk assessments and due diligence, contracting, ongoing oversight and management of the third party relationship, and escalating third party issues to senior management. Corporate Compliance serves as the second line of defense and is responsible for working with the business lines and the Corporate Vendor Management Office to ensure that vendor relationships are evaluated and monitored in compliance with federal guidelines and Bank policies and procedures.
BOKF's ability to assess, monitor, and mitigate risks from its use of subcontractors and to ensure that the same level of quality and controls exists no matter where the subcontractors' operations reside.	BOKF utilizes standardized third party risk assessments to consistently review and assess third party risk. This assessment is initially completed when a third party is first engaged by BOKF. Assessments are updated annually for high risk relationships and every two years for medium risk relationships to identify any material changes to the third party relationship. BOKF reviews due diligence documentation for Information Security, Business Continuity, Physical Security and Compliance risks in addition to performing onsite investigations where warranted, commensurate with the type of risk identified in the assessment. Performance scorecards are used to monitor third party performance based on risk. Deviations from BOKF standards in any of the above risk reviews or performance evaluations is reported and escalated to senior management.

[i] From New Employee Welcome Center site
[ii] Annual report
[iii] Annual report
[iv] From New Employee Welcome Center site
[v] Corporate Compliance Management Policy