



Compliance Alliance Due Diligence Packet

Updated 04.04.2024

Table of Contents

| | |
|--|-------|
| Company Overview | 3-10 |
| Our Story..... | 3 |
| ▪ Compliance Hub | 4 |
| ▪ Assurance Services | 5-6 |
| ▪ Virtual Partners | 6-7 |
| Our Leadership..... | 8-9 |
| Board of Directors | 10 |
| Insurance | 11 |
| Financials..... | 12-26 |
| Privacy Policy..... | 27-30 |
| IT..... | 31-63 |
| ▪ TBA Incident Recovery Plan | 31-32 |
| ▪ TBA IT Disaster Recovery Plan..... | 33-37 |
| ▪ TBA IT Security Posture - February 2024..... | 38-46 |
| ▪ TBA Security Policy..... | 47-50 |
| ▪ TBA Security Controls..... | 51-54 |
| ▪ TBA IT BYOD Policy | 55-56 |
| ▪ Cyber Hygiene Report- February 2024..... | 57 |
| ▪ Citrix Systems Soc 2 Report..... | 58 |
| ▪ Microsoft 365 Assessment..... | 59-63 |

Our Story

Our journey began in 2010, driven by the enactment of Dodd-Frank, which created a vital need for State Bankers Associations to assist their community bank members grappling with a surge of regulatory challenges. By 2011, the State Bankers Associations had responded to the industry's challenges by creating Compliance Alliance which aimed to address the needs of banks overwhelmed with frequent examinations and the new regulations.

As Compliance Alliance emerged, it became clear that our unwavering commitment to craft programs specifically tailored to the dynamic regulatory landscape while addressing the unique needs of community banks must continue. Over time, this initiative evolved into a comprehensive suite of services that includes Compliance Hub, Assurance Services, and Virtual Partners.

Established in partnership with 16 initial State Bankers Associations, Compliance Alliance's services were designed to go beyond those offered by endorsed partners, taking a lead role in guiding member banks through the quickly changing regulatory landscape. Today, Compliance Alliance supports community banks nationwide as they navigate the complexities of regulatory compliance best practice.

Compliance Alliance has emerged as the foremost compliance service provider for community banks nationwide. Ownership is vested in 36 State Bankers Associations, and our Board of Directors includes the President/CEO or their designee from each of these associations. Collectively, the 36 State Bankers Associations own 100% of the company shares and All profits generated benefit these associations. C/A's esteemed board guides our affairs, setting policies, objectives, and overseeing Bankers Alliance's management, while playing a pivotal role in shaping the direction of compliance services for member banks.

Continuing its responsive approach, Compliance Alliance created Assurance Services in 2018, a review (audit) company, while also advancing community bank-minded programs. In 2020, we introduced Virtual Partners - the revolutionary Virtual Compliance Officer (VCO) program. This compliance management innovation integrates Virtual Compliance Officers at the community bank-level, revolutionizing compliance management, and ensuring a cohesive and adaptive response to regulatory challenges.

At the heart of Compliance Alliance is a reputation forged as the premier provider of compliance services exclusively tailored for banks. Our team, led by attorneys, former bankers, and regulators, brings a wealth of experience to assist community banks nationwide in addressing the most pressing compliance and regulatory issues. With over 500 years of combined experience, our expert team holds various certifications, including CRCM, CCBCO, CCBTO, CCBIA, CBAP, CIA, CIPP, AAP, and CERP.

Compliance Hub

Compliance Hub raises the bar by uncovering new ways to assist with federal regulatory compliance within your financial institution. Membership-based with unlimited access, Compliance Hub is the solution designed for the whole bank; from the Board of Directors to Operations.

Compliance Hub: A Pioneer in Community Banking Compliance

Established in 2011, Compliance Hub stands out as the sole banking industry compliance resource owned, operated, and managed by 36 State Bankers Associations.

Comprehensive Services

Addressing the specific needs of community bankers, Compliance Hub offers an all-encompassing suite of bank compliance tools and services, ensuring members stay abreast of consumer and regulatory requirements.

Key Offerings:

- **All-Access Hotline:** Members benefit from immediate assistance for regulatory and consumer compliance queries through our hotline, available from 7 AM to 6:00 PM Central time via phone, email, or live chat.
- **Document Reviews:** Gain peace of mind with our in-house experts conducting thorough document reviews, providing recommendations within three business days. Unlimited reviews allow for iterative improvements ensuring full compliance.
- **Library of Compliance Tools:** Access an extensive array of editable tools and services, including calculators, cheat sheets, checklists, compliance calendars, flowcharts, forms, handouts, huddles, matrices, podcasts, policies, procedures, risk assessments, signage, summaries, training tools, videos, webinars, worksheets, and more. Custom tools are created at no extra cost upon request.
- **Easy Access to Regulations:** Navigate federal and state regulatory information effortlessly on the Compliance Alliance website. The hotline is available to assist with federal research as needed.
- **Summaries of New Regulations:** Our legal experts provide concise, layman's term summaries of new regulations, offering clarity on how changes impact banks along with actionable implementation plans.
- **Regular Updates on Regulations:** Stay informed with daily, weekly, and monthly emails providing crucial news, overviews of added tools, and comprehensive information about regulatory requirements and changes.
- **Compliance Huddles:** Our *Compliance Huddles* facilitate discussions among compliance professionals nationwide, addressing hot topics, recent examinations, and general compliance concerns. These sessions, moderated by Compliance Hub's experts, also serve as valuable networking opportunities for member banks.
- **Membership Insights:** Participate in our live demos to experience the program's benefits firsthand. Our annual membership fee includes unlimited access to all products and services for every employee of subscribing banks, making Compliance Alliance the most unique and cost-effective, banking compliance resource in the market today.

Assurance Services

Assurance Services: Elevating Banking Audits with On-Time Delivery

When it comes to comprehensive bank audits and reviews, Assurance Services is your trusted partner, providing experience, a meticulous audit process, and consistent timely reporting that ensures your institution is on the right track.

Why Assurance Services?

Each of our bank auditors have successfully navigated hundreds, if not thousands, of both internal and external bank reviews and audits. We understand the intricacies of preparation and excel in steering necessary course corrections for optimal outcomes.

- **BSA/AML Compliance Review: 5 Pillar Review:** A thorough examination covering Officer Designation, Customer Due Diligence, Independent Testing, Training, and Policies, Procedures, Monitoring, and Controls.
- **Deposit Compliance Review:**
 - Truth in Savings: Ensuring accuracy and compliance.
 - Privacy of Consumer Financial Information: Safeguarding consumer data.
 - Electronic Banking and Fund Transfers: Assessing compliance with electronic banking regulations.
 - Expedited Funds Availability: Ensuring adherence to fund availability regulations.
 - Interests on Deposits: Reviewing interest practices.
 - Unlawful Internet Gambling: Compliance assessment.
 - NOW Account and MMDA: Examination of compliance in these account types.
- **Lending Compliance Review:**
 - Truth in Lending: Assessing transparency in lending practices.
 - TRID (TILA-RESPA Integrated Disclosure): Compliance with disclosure regulations.
 - Homeowners Protection: Ensuring compliance with mortgage insurance cancellation.
 - Homeownership Counseling: Assessing adherence to homeownership counseling requirements.
 - Credit Practices Rule and Equal Credit Opportunity: Ensuring fair lending practices.
 - Fair Housing: Compliance with fair housing regulations.
 - Home Mortgage Disclosure Act (HMDA): Scrutinizing HMDA compliance.
 - Fair Credit Reporting & Fact: Reviewing practices related to credit reporting.
 - Flood Insurance: Compliance with flood insurance regulations.
 - Privacy: Ensuring privacy policy compliance.
- **ACH Compliance Review:**
 - Policies, Procedures, Training, Agreements, Records, Retention, Prenotes, NOCs, Returns, Stop Payments, Disclosures: A comprehensive assessment of ACH practices.

- **Internal Control Review:**
 - Adequacy of Internal Controls: Evaluating the effectiveness of internal controls.
 - Compliance with Procedures: Ensuring adherence to established procedures.
 - Review of the Operation: A holistic examination of operational processes.
 - Teller Cash, Vault Cash, Monetary Instrument Reconciliation, Dual Control Logs: Scrutinizing key control points.
- **Special Project Reviews:**
 - MSB Monitoring and Reporting: Ensuring compliance with regulations related to Money Service Businesses.
 - Private Flood Policy Review – Pre-Closing and Post-Delivery: Assessing adherence to private flood policy requirements.
 - HMDA Scrubs and LAR Review and Reporting: Comprehensive reviews and reporting for HMDA compliance.
 - MRB Monitoring and Reporting: Compliance assessments related to Marijuana-Related Businesses.

In choosing Assurance Services, you opt for a partner committed to excellence in every facet of banking compliance, helping to ensure your institution is well-prepared and resilient in the face of regulatory scrutiny.

Virtual Partners

Virtual Compliance Officer (VCO): Driving Regulatory Excellence

As the regulatory landscape changed, our innovative remote compliance management approach—Virtual Compliance Officers (VCOs)—have revolutionize compliance management, ensuring a cohesive and adaptive response to regulatory challenges and the demands on banking staff.

Key Functions of Virtual Compliance Officers (VCOs):

- **Staff Augmentation and Seamless Integration:** VCOs seamlessly integrate into your team, offering crucial support during transitional periods and ensuring a smooth compliance transition.
- **Outsourced Monitoring and Reporting:** Entrust VCOs with ongoing monitoring and reporting responsibilities, allowing internal resources to focus on core business activities. VCOs specialize in creating formalized, comprehensive reports that withstand regulatory scrutiny.
- **Tailored CMS Programs and Continuous Compliance Improvement:** Leverage VCOs' expertise to build customized Compliance Management System (CMS) programs. Beyond oversight, VCOs provide valuable observations and actionable items for continuous compliance improvement.
- **Collaboration and Knowledge Transfer:** Work directly with VCOs as they integrate into your team by fostering effective communication and knowledge transfer for a cohesive compliance environment.
- **Expertise Management and Regulatory Advisory:** Our VCOs maintain advanced expertise on laws and regulations and **provide a regular advisory on compliance expectations from regulatory bodies.**
- **Comprehensive Compliance Program and Policy Development:** **VCOs implement and manage a robust compliance program that aligns with best practices and assists in the development and review of bank policies and procedures.**
- **BSA Program Oversight and Action Plan Development:** Manage compliance with the bank's BSA Program and create effective action plans in response to audit findings and compliance violations.

- **Risk Assessment and Control System Efficiency:** Assess company operations for compliance risk and regularly evaluate the efficiency of control systems, recommending improvements.
- **Procedure and Documentation Review and Committee Leadership:** Review company procedures, reports, and compliance-related documentation. Chair the Compliance Committee and/or BSA Committee, **while** actively participating in key governance forums.

Suite 16 Program

Designed to cater to community banks' specific regulatory needs, the Suite 16 program provides a dedicated compliance or BSA officer. This officer offers expertise in Community Reinvestment Act (CRA), Home Mortgage Disclosure Act (HMDA), Unfair and Deceptive Acts and Practices (UDAAP), Fair Lending laws, Deposit or Lending Compliance, or the Bank Secrecy Act (BSA), based on your requirements.

Responsibilities may include:

- **Expertise Maintenance:** Maintain advanced knowledge of various laws, regulations, and rulings.
- **Procedure Adequacy and Advisory:** Review and advise on the adequacy of procedures related to data collection, fair lending, and UDAAP.
- **New Product and Service Compliance:** Provide feedback during new or revised product, service, or market development to ensure compliance.
- **Committee Attendance and CRA Maintenance:** Attend relevant committees, manage aspects of CRA maintenance, and provide guidance on technical aspects of CRA and HMDA regulations.
- **Performance Reporting and Compliance Oversight:** Report the status of CRA, HMDA, Fair Lending, and BSA performance and compliance to management and the Board.
- **Regulatory Exam Support:** Assist in regulatory exams, internal and external audits, and compliance monitoring reviews.
- **Data Integrity Reviews and BSA Oversight:** Conduct CRA and HMDA Data Integrity Reviews and oversee the Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Office of Foreign Assets Control (OFAC) programs.
- **Suspicious Activity Monitoring and Reporting:** Oversee the monitoring of account activity for suspicious patterns, conduct suspicious activity report (SAR) investigations, and decide when to file suspicious activity reports.
- **Risk Assessments and Action Plan Management:** Prepare risk assessments and create/manage action plans in response to audit and exam discoveries and compliance violations.

The Virtual Partners compliance management approach provides a seamless blend of expertise, technology, and strategic oversight, ensuring your organization is well-equipped to navigate transitions, optimize monitoring and reporting, and build tailored programs for regulatory excellence and operational resilience.

Leadership at Compliance Alliance:

Scott Daugherty - President & General Counsel, Compliance Alliance

Scott Daugherty serves as the dynamic President & General Counsel for Compliance Alliance, steering the strategic direction of the organization and its business lines - Virtual Partners, and Assurance Services. With a rich background in banking and legal expertise, Scott's visionary leadership led to the conceptualization and establishment of Compliance Alliance in 2011.

Scott's illustrious career spans roles in retail and branch management, consumer and commercial lending, and significant service on the legal staff of the Texas Bankers Association. As one of the nation's foremost experts in bank regulatory compliance and law, Scott is not only a seasoned professional, but also a sought-after speaker and contributor to banking publications. His insights have played a pivotal role in shaping Compliance Alliance and helped make it the premier bank compliance service in the industry.

Beyond Compliance Alliance, Scott has been a pivotal figure since founding Assurance Services in 2018 and Virtual Partners in 2020. As one of the driving forces behind these initiatives, Scott continues to oversee the creation and dissemination of advisory services through Compliance Alliance. Simultaneously, he guides the growth and development of Assurance Services and the Virtual Partners program, helping to extend its reach to banks across the nation and at every level.

A passionate advocate for the banking industry, Scott collaborates closely with elected officials, effectively conveying the legislative impact on the industry and, by extension, the community. His unwavering commitment to excellence and strategic vision continues to elevate Compliance Alliance and its subsidiaries to new heights in the financial services landscape.

Chance Williams – Executive Vice President, Virtual Partners

Holding certifications in Audit, BSA, Compliance, and IT, Chance Williams is the Executive Vice President, Virtual Partners. With a wealth of compliance expertise, Chance's career includes roles as a Compliance Officer and Auditor, contributing to Business Development Teams, Loan Committees, and various committees liaising with regulatory agencies. His extensive experience, spanning 17 years as a compliance officer/auditor and 8 years as a senior compliance/audit consultant, positions him as a valuable asset in strengthening bank compliance management systems.

Chance has been a pivotal figure since the founding of Assurance Services in 2018 and Virtual Partners in 2020. As one of the driving forces behind these initiatives, he continues to oversee the Virtual Partners program, helping to extend its reach to banks across the nation and at every level.

Chance's contributions extend to speaking at conventions, meetings, and schools, along with articles in state banking association magazines and Compliance Alliance's newsletters. His focus on enhancing compliance aligns with Compliance Alliance's commitment to excellence.

Amanda Mattson, CCBIA, CCBCO – Executive Vice President, Assurance Services

Amanda Mattson, CCBIA, CCBCO, brings nearly two decades of comprehensive financial industry experience to her role as the Executive Vice President Assurance Services Holding certifications in both Audit (CCBIA) and Compliance (CCBCO), Amanda is a Certified Bank Auditor, demonstrating her commitment to excellence in the field.

Originally from Northern Michigan, Amanda earned her Bachelor's degree in Business Administration from Lake Superior State University. She is a proud contributor to Compliance Alliance Access magazine, showcasing her expertise in the financial industry.

Amanda's diverse career encompasses roles in lending and retail banking. She served as a Vice President/Branch Manager for prominent institutions such as Citi, JPMorgan Chase, and Bank of the West. Her extensive knowledge in community bank compliance extends to various facets, including branch compliance, collections and solicitations, credit decisions, foreclosures, closed loans, and more.

In addition to her operational roles, Amanda has actively contributed to the development of internal procedures and disclosures, showcasing her dedication to maintaining high standards in banking practices. Her commitment to community development is evident through providing FDIC Financial Education classes in local schools.

Amanda Mattson's multifaceted experience and certifications make her an invaluable asset to Assurance Services, where her leadership in audit operations contributes to the company's commitment to excellence in compliance and regulatory adherence.

Victoria E. Stephen, JD, CRCM - Executive Vice President & General Counsel, Compliance Hub

Victoria Stephen serves as Executive Vice President & General Counsel, for Compliance Hub. Since joining in 2015, she has played a crucial role in leading the hotline attorneys and compliance officers, developing new products, and providing internal and external training. A licensed attorney in Texas, Victoria's career has included consulting for some of the nation's largest banks on regulatory risk, compliance, and controls.

Victoria's passion for banking and compliance developed during an internship with a community bank, and she continued to pursue these interests at The University of Texas School of Law. Her contributions include speaking at compliance conferences, schools, and writing for national and state banker publications. Victoria's experience and leadership contribute significantly to Compliance Hub's impact on the banking industry.

Executive Committee

Rann Paynter - President & Chief Executive Officer, Michigan Bankers Association Richard Baier – President & Chief Executive Officer, Nebraska Bankers Association
Kristy Merrill – President, New Hampshire Bankers Association
Linda Navaro - President & Chief Executive Officer Oregon Bankers Association
Colin Barret - President & Chief Executive Officer Tennessee Bankers Association
Chris Furlow - President & Chief Executive Officer Texas Bankers Association
Bruce Whitehurst - President & Chief Executive Officer, Virginia Bankers Association

Board of Directors

Scott Latham - President & Chief Executive Officer, Alabama Bankers Association
Lorrie Trogden - President & Chief Executive Officer, Arkansas Bankers Association
Paul Hickman - President & Chief Executive Officer, Arizona Bankers Association
Kevin Gould - President & Chief Executive Officer, California Bankers Association
Jenifer Waller - President & Chief Executive Officer, Colorado Bankers Association Thomas
Mongellow - President & Chief Executive Officer, Connecticut Bankers Association Alex Sanchez -
President & Chief Executive Officer, Florida Bankers Association
Bo Brannen - Senior Vice President, Georgia Bankers Association
Trent Wright - President & Chief Executive Officer, Idaho Bankers Association
Rod Lasley – Chief Operating Officer, Indiana Bankers Association
Ballard Cassady - President & Chief Executive Officer, Kentucky Bankers Association Ginger Laurent -
President & Chief Executive Officer, Louisiana Bankers Association Ramon Looby - President & Chief
Executive Officer, Maryland Bankers Association Kathleen Murphy - President & Chief Executive
Officer, Massachusetts Bankers Association Rann Paynter - President & Chief Executive Officer,
Michigan Bankers Association Gordon Fellows - President & Chief Executive Officer, Mississippi
Bankers Association Sam Sill - President & Chief Executive Officer, Montana Bankers Association
Richard Baier – President & Chief Executive Officer, Nebraska Bankers Association
Phyllis Gurgevich - President & Chief Executive Officer, Nevada Bankers Association Kristy Merrill –
President, New Hampshire Bankers Association
John Anderson Executive Vice President, New Mexico Bankers Association
Peter Gwaltney - President & Chief Executive Officer, North Carolina Bankers Association Rick
Clayburgh - President & Chief Executive Officer, North Dakota Bankers Association Mike Adelman -
President & Chief Executive Officer, Ohio Bankers League
Adrian Beverage - President & Chief Executive Officer, Oklahoma Bankers Association Linda Navaro -
President & Chief Executive Officer Oregon Bankers Association
Duncan Campbel - President & Chief Executive Officer, Pennsylvania Bankers Association Karlton
Adam - President & Chief Executive Officer, South Dakota Bankers Association Colin Barret -
President & Chief Executive Officer Tennessee Bankers Association
Chris Furlow - President & Chief Executive Officer Texas Bankers Association
Howard Headlee - President & Chief Executive Officer, Utah Bankers Association
Bruce Whitehurst - President & Chief Executive Officer, Virginia Bankers Association Glen Simecek -
President & Chief Executive Officer, Washington Bankers Association Mark Mangano - President &
Chief Executive Officer, West Virginia Bankers Association



TBA and Subsidiaries Financial Report



Consolidated Financial Statements
May 31, 2023 and 2022

The Bank Store, Inc. and Subsidiary

| | |
|---|---|
| Independent Auditor’s Report | 1 |
| Consolidated Financial Statements | |
| Consolidated Balance Sheets | 3 |
| Consolidated Statements of Operations..... | 4 |
| Consolidated Statements of Stockholders’ Equity (Deficit) | 5 |
| Consolidated Statements of Cash Flows | 6 |
| Notes to Consolidated Financial Statements..... | 7 |



Independent Auditor's Report

To the Board of Directors
The Bank Store, Inc. and Subsidiary
Austin, Texas

Report on the Audit of the Consolidated Financial Statements

Opinion

We have audited the consolidated financial statements of The Bank Store, Inc. and Subsidiary, which comprise the consolidated balance sheets as of May 31, 2023 and 2022, and the related consolidated statements of operations, stockholders' equity (deficit), and cash flows for the years then ended, and the related notes to the consolidated financial statements.

In our opinion, the accompanying consolidated financial statements referred to above present fairly, in all material respects, the financial position of The Bank Store, Inc. and Subsidiary as of May 31, 2023 and 2022, and the results of its operations and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Basis for Opinion

We conducted our audits in accordance with auditing standards generally accepted in the United States of America (GAAS). Our responsibilities under those standards are further described in the Auditor's Responsibilities for the Audit of the Consolidated Financial Statements section of our report. We are required to be independent of The Bank Store, Inc. and Subsidiary and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Responsibilities of Management for the Consolidated Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with accounting principles generally accepted in the United States of America; and for the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the consolidated financial statements, management is required to evaluate whether there are conditions or events, considered in the aggregate, that raise substantial doubt about The Bank Store, Inc. and Subsidiary's ability to continue as a going concern for one year after the date that the consolidated financial statements are available to be issued.

Auditor's Responsibilities for the Audit of the Consolidated Financial Statements

Our objectives are to obtain reasonable assurance about whether the consolidated financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the consolidated financial statements.

In performing an audit in accordance with GAAS, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the consolidated financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of The Bank Store, Inc. and Subsidiary's internal control. Accordingly, no such opinion is expressed.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the consolidated financial statements.
- Conclude whether, in our judgment, there are conditions or events, considered in the aggregate, that raise substantial doubt about The Bank Store, Inc. and Subsidiary's ability to continue as a going concern for a reasonable period of time.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control–related matters that we identified during the audit.



Abilene, Texas
August 28, 2023

The Bank Store, Inc. and Subsidiary

Consolidated Balance Sheets

May 31, 2023 and 2022

| Assets | 2023 | 2022 |
|---|---------------------|---------------------|
| Current assets | | |
| Cash and cash equivalents | \$ 1,369,375 | \$ 1,746,196 |
| Accounts receivable - trade | 21,212 | 15,285 |
| Accounts receivable - related parties | 862,707 | 752,638 |
| Federal income tax receivable | 80,961 | - |
| Other current assets | 569,824 | 481,353 |
| Total current assets | <u>2,904,079</u> | <u>2,995,472</u> |
| Noncurrent assets | | |
| Deferred tax asset | 51,447 | 45,189 |
| Total noncurrent assets | <u>51,447</u> | <u>45,189</u> |
| Total assets | <u>\$ 2,955,526</u> | <u>\$ 3,040,661</u> |
| Liabilities and Stockholders' Deficit | | |
| Current liabilities | | |
| Accounts payable and accrued liabilities | \$ 298,865 | \$ 354,913 |
| Accounts payable - related parties | 38,223 | 409,769 |
| Federal income tax payable | - | 7,732 |
| Deferred revenue | 3,211,686 | 3,024,277 |
| Total current liabilities | <u>3,548,774</u> | <u>3,796,691</u> |
| Total liabilities | <u>3,548,774</u> | <u>3,796,691</u> |
| Stockholders' deficit | | |
| Retained deficit | (1,096,026) | (1,251,609) |
| Noncontrolling interests | 502,778 | 495,579 |
| Total stockholders' deficit | <u>(593,248)</u> | <u>(756,030)</u> |
| Total liabilities and stockholders' deficit | <u>\$ 2,955,526</u> | <u>\$ 3,040,661</u> |

The Bank Store, Inc. and Subsidiary
Consolidated Statements of Operations
Years Ended May 31, 2023 and 2022

| | <u>2023</u> | <u>2022</u> |
|---|--------------------------|--------------------------|
| Operating Revenues | | |
| Products and services | <u>\$ 5,578,954</u> | <u>\$ 5,432,897</u> |
| Operating Expenses | | |
| Royalties | 980,131 | 909,068 |
| Other direct expenses | 333,104 | 330,133 |
| Employee costs | 1,957,393 | 1,771,950 |
| General office | 196,712 | 191,325 |
| Staff travel | 113,420 | 109,458 |
| Professional services | 31,795 | 33,628 |
| Administrative expense | 1,283,935 | 1,246,444 |
| Other | <u>170,420</u> | <u>281,006</u> |
| Total operating expenses | <u>5,066,910</u> | <u>4,873,012</u> |
| Operating income | <u>512,044</u> | <u>559,885</u> |
| Other Income (Expense) | | |
| Investment income | 80 | 31,679 |
| Net realized and unrealized loss on investments | <u>-</u> | <u>(44,659)</u> |
| Total other income (expense) | <u>80</u> | <u>(12,980)</u> |
| Net income before income taxes | 512,124 | 546,905 |
| Provision for income taxes | <u>(112,541)</u> | <u>(114,306)</u> |
| Net income | 399,583 | 432,599 |
| Net loss attributable to noncontrolling interests | <u>6,000</u> | <u>3,446</u> |
| Net income attributable to the Company | <u><u>\$ 405,583</u></u> | <u><u>\$ 436,045</u></u> |

The Bank Store, Inc. and Subsidiary
Consolidated Statements of Stockholders' Equity (Deficit)
Years Ended May 31, 2023 and 2022

| | Retained Earnings (Deficit) | Non- controlling Interest | Total Stockholders' Equity (Deficit) |
|--|-----------------------------------|---------------------------------|--|
| Balance, May 31, 2021 | \$ 1,352,242 | \$ 457,775 | \$ 1,810,017 |
| Issuance of common stock | - | 41,250 | 41,250 |
| Net loss attributable to noncontrolling interest | - | (3,446) | (3,446) |
| Dividends paid | (3,039,896) | - | (3,039,896) |
| Net income attributable to the Company | 436,045 | - | 436,045 |
| Balance, May 31, 2022 | <u>\$ (1,251,609)</u> | <u>\$ 495,579</u> | <u>\$ (756,030)</u> |
| Issuance of common stock | - | 13,199 | 13,199 |
| Net loss attributable to noncontrolling interest | - | (6,000) | (6,000) |
| Dividends paid | (250,000) | - | (250,000) |
| Net income attributable to the Company | 405,583 | - | 405,583 |
| Balance, May 31, 2023 | <u>\$ (1,096,026)</u> | <u>\$ 502,778</u> | <u>\$ (593,248)</u> |

The Bank Store, Inc. and Subsidiary
Consolidated Statements of Cash Flows
Years Ended May 31, 2023 and 2022

| | <u>2023</u> | <u>2022</u> |
|--|---------------------|---------------------|
| Operating Activities | | |
| Net income | \$ 399,583 | \$ 432,599 |
| Adjustments to reconcile net income to net cash from operating activities | | |
| Deferred income tax | (6,258) | (84,882) |
| Net realized and unrealized loss (gain) on investments | - | 44,659 |
| Net change in | | |
| Accounts receivable - trade | (5,927) | (15,285) |
| Accounts receivable - related parties | (110,069) | (749,429) |
| Federal income tax receivable | (80,961) | - |
| Other current assets | (88,471) | 13,399 |
| Accounts payable and accrued liabilities | (56,048) | 22,975 |
| Accounts payable - related parties | (371,546) | 153,222 |
| Federal income tax payable | (7,732) | (12,897) |
| Deferred revenue | 187,409 | (34,991) |
| Net Cash used for Operating Activities | <u>(140,020)</u> | <u>(230,630)</u> |
| Investing Activities | | |
| Purchase of marketable securities | - | (4,537,485) |
| Proceeds from sale of marketable securities | - | 6,456,914 |
| Net Cash from Investing Activities | <u>-</u> | <u>1,919,429</u> |
| Financing Activities | | |
| Issuance of common stock | 13,199 | 41,250 |
| Dividends paid | (250,000) | (3,039,896) |
| Net Cash used for Financing Activities | <u>(236,801)</u> | <u>(2,998,646)</u> |
| Net Change in Cash and Cash Equivalents | (376,821) | (1,309,847) |
| Cash and Cash Equivalents, Beginning of Year | 1,746,196 | 3,056,043 |
| Cash and Cash Equivalents, End of Year | <u>\$ 1,369,375</u> | <u>\$ 1,746,196</u> |
| Supplemental Disclosure of Cash Flow Information | | |
| Cash payments for Income taxes | <u>\$ 207,492</u> | <u>\$ 212,629</u> |

Note 1 - Summary of Significant Accounting Policies

A summary of significant accounting policies consistently applied in the preparation of the accompanying consolidated financial statements follows:

Principles of Consolidation

The accompanying consolidated financial statements include the accounts of The Bank Store, Inc. (TBS), a taxable entity, and its majority owned for-profit subsidiary, Compliance Alliance, Inc. (CAI).

At May 31, 2023 and 2022, The Bank Store, Inc. owns 100% of the outstanding 100,000 shares of CAI Class A voting stock and the remaining ownership is treated as noncontrolling interest in these consolidated financial statements (see Note 4).

All significant intercompany accounts and transactions have been eliminated in consolidation.

Company and Nature of Business

The Bank Store, Inc. and Subsidiary (the Company), Compliance Alliance, Inc., were formed as federal taxable entities. The banking industry is driven by laws, regulations and rules mandated by both the federal and state governments. Regulatory compliance is a time-consuming burden for banks. Rules, regulations and laws change frequently, and it is difficult to keep up with and apply the rules and regulations to the bank's operations. In response to the need for help, the Company was formed to increase the effectiveness of banks' compliance programs and to facilitate broad industry initiatives directed at addressing a variety of compliance functions for member banks and concerns of common interest. The primary goal of the Company is to provide quality compliance services and free up the banks' compliance personnel to focus on bank-specific functions. The Bank Store, Inc. focuses on offering services within Texas while Compliance Alliance, Inc. offers services to financial institutions outside of Texas through its association with banking associations.

Cash and Cash Equivalents

Cash and cash equivalents consist of cash in banks and all short-term highly liquid investments with original maturities of three months or less.

Concentration of Credit Risk

The Company places its cash and cash equivalents with high quality financial institutions, which at times may exceed federally insured limits. The Company has not experienced any losses on such accounts. At May 31, 2023 and 2022, bank deposits in excess of federally insured limits were \$869,375 and \$1,246,196, respectively.

Common Stock

The subsidiary, Compliance Alliance, Inc., has authorized a total of 200,000 shares of common stock. The shares are classified as 100,000 shares designated Class A Voting Common Stock which can only be purchased by The Bank Store, Inc. who has been issued all Class A shares, and 100,000 shares designated Class B Non-Voting Common Stock, which can be issued to other state banking associations. As of May 31, 2023 and 2022, 3,501 and 3,413 shares of Class B Non-Voting Common Stock, respectively, have been issued. Compliance Alliance, Inc. has purchased 15,000 shares of Treasure Stock as of May 31, 2023 and 2022. The Bank Store, Inc., operates as a nonstock corporation.

Income Taxes

The Company is classified for income tax purposes as a C-Corporation and files a consolidated tax return. Income taxes are provided for the tax effects of transactions reported in the consolidated financial statements and consist of taxes currently due plus deferred taxes related primarily to differences between the basis of accrued expenses. The deferred tax asset represents the future tax return consequences of those differences, which will be deductible when the asset or liability is recovered or settled.

Deferred tax assets are reduced by a valuation allowance when, in the opinion of management, it is more likely than not that some portion of the deferred tax asset will not be realized. As of May 31, 2023 and 2022, management has not applied a valuation allowance, because it believes the full deferred tax asset will be realized.

The Company evaluates its tax positions that have been taken or are expected to be taken on income tax returns to determine if an accrual is necessary for uncertain tax positions. As of May 31, 2023 and 2022, the unrecognized tax benefits accrual was zero. The Company will recognize future accrued interest and penalties related to unrecognized tax benefits in income tax expense if incurred. During the years ended May 31, 2023 and 2022, the Company recognized no interest and penalties.

In May of 2006, the State of Texas implemented a tax on taxable margin, effective for years ended after December 31, 2006. For the Company, taxable margin is revenue less interest expense. The margin tax is insignificant for the years ended May 31, 2023 and 2022 and is included in other expenses in the consolidated financial statements.

Sales Taxes

Various states impose a sales tax on the Company's sales to non-exempt customers. All sales taxes collected by the Company are remitted to the appropriate states. The Company's accounting policy is to exclude the tax collected and remitted to the states from revenue and expenses.

Advertising Costs

Advertising costs are expensed as incurred. Such costs were \$23,131 and \$22,227 for the years ended May 31, 2023 and 2022, respectively.

Revenue Recognition

The Company earns revenue through selling subscriptions for compliance product services. Revenue is recognized over the period in which the Company provides the services. Fees collected in advance are amortized over the subscription year or the period that services are provided.

Use of Estimates

In preparing consolidated financial statements in conformity with accounting principles generally accepted in the United States of America, management is required to make estimates and assumptions that affect the reported amounts of assets and liabilities and the disclosure of contingent assets and liabilities at the date of the consolidated financial statements and the reported amounts of revenues and expenses during the reporting period. Actual results could differ from those estimates.

Subsequent Events

The Company has evaluated all subsequent events through August 28, 2023, the date the consolidated financial statements were available to be issued.

Note 2 - Related Party Transactions

The Company is closely affiliated and controlled by Texas Bankers Association (TBA), a not-for-profit organization. TBA facilitates substantially all accounting and recordkeeping functions for the Company. The Company paid management fees directly to TBA for the years ended May 31, 2023 and 2022 totaling \$592,092 and \$536,609, respectively. Expenses paid by TBA on behalf of the Company are reimbursed to TBA on a monthly basis and are properly categorized in the Company's consolidated financial statements.

As of May 31, 2023 and 2022, the Company had accounts receivable from TBA of \$862,707 and \$752,638, respectively, as TBA temporarily borrowed cash for building construction. As of May 31, 2023 and 2022, the Company had accounts payable to TBA of \$38,223 and \$409,769, respectively.

The employees of the Company are eligible to participate in a qualified retirement plan (401(k)) sponsored by TBA. Amounts reimbursed to TBA amounted to \$128,026 and \$104,100 for the years ended May 31, 2023 and 2022, respectively.

Note 3 - Income Taxes

The income tax expense recognized for the years ended May 31, 2023 and 2022, consists of the following:

| | 2023 | 2022 |
|-------------------------------------|------------|------------|
| Current federal income tax expense | \$ 118,799 | \$ 199,188 |
| Deferred federal income tax benefit | (6,258) | (84,882) |
| | \$ 112,541 | \$ 114,306 |

Deferred tax assets and liabilities consist of the following components as of May 31, 2023 and 2022:

| | 2023 | 2022 |
|-------------------------|-----------|-----------|
| Deferred tax assets | | |
| Accrued paid time off | \$ 13,926 | \$ 12,488 |
| Charitable contribution | 36,947 | 28,178 |
| Deferred revenue | 574 | 4,523 |
| Net deferred tax asset | \$ 51,447 | \$ 45,189 |

Net deferred tax assets are presented as a noncurrent asset and net deferred tax liabilities are presented as a long-term liability in the accompanying consolidated balance sheets.

Note 4 - Noncontrolling Interest in Subsidiary

On September 20, 2011, Compliance Alliance, Inc., (CAI) was formed as a taxable entity. The company was formed for the purpose of providing compliance services to member banks of other state banking associations in response to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Compliance services continue to expand as regulations are introduced by banking regulatory agencies. Member banks within the respective states may subscribe to CAI services.

TBS owns 100% of the outstanding 100,000 shares of Class A voting stock and exercises control over CAI. Due to its relationship, there is a noncontrolling interest associated with the equity shares not owned by TBS. Therefore, the assets, liabilities, and transactions of CAI have been consolidated into the financial statements of TBS for the years ended May 31, 2023 and 2022. The noncontrolling ownership interest is included as a separate component of stockholders' equity on those consolidated financial statements and designated in the stockholders' equity of The Bank Store, Inc. and Subsidiary.

Assets of CAI that are included in the consolidated balance sheets of TBS at May 31, 2023 and 2022 consist of:

| | <u>2023</u> | <u>2022</u> |
|---------------------------------------|-------------|--------------|
| Cash and cash equivalents | \$ 773,827 | \$ 1,144,613 |
| Federal income tax receivable | 224,363 | 177,483 |
| Accounts receivable - trade | 21,212 | 15,285 |
| Accounts receivable - related parties | 744,332 | 752,638 |
| Prepaid royalties | 553,925 | 466,569 |
| Deferred tax asset | 10,861 | 11,223 |

Liabilities of CAI that are included in the consolidated balance sheets of TBS at May 31, 2023 and 2022 consist of:

| | <u>2023</u> | <u>2022</u> |
|---|-------------|-------------|
| Accounts payable and other accrued expenses | \$ 221,107 | \$ 260,059 |
| Accounts payable - related parties | 38,223 | 315,232 |
| Deferred revenue | 2,384,052 | 2,141,275 |

The following expenses were paid from CAI to TBS and were eliminated upon consolidation:

| | <u>2023</u> | <u>2022</u> |
|-----------|-------------|-------------|
| Royalties | \$ 399,470 | \$ 380,383 |

Note 5 - Revenue From Contracts with Customers

Substantially all of the Company's revenue is recognized over time. Revenue from performance obligations satisfied over time consists of the sale of compliance products and services through one-year and three-year contracts sold to member banks.

Deferred revenues are contract liabilities for billings in excess of revenue recognized. The beginning and ending balances for accounts receivable and deferred revenue were as follows at May 31:

| | <u>2023</u> | <u>2022</u> | <u>2021</u> |
|-----------------------------|---------------------|---------------------|---------------------|
| Accounts receivable - trade | <u>\$ 21,212</u> | <u>\$ 15,285</u> | <u>\$ -</u> |
| Deferred revenue | <u>\$ 3,211,686</u> | <u>\$ 3,024,277</u> | <u>\$ 3,059,268</u> |

Note 6 - Employee Benefit Plan

The Bank Store, Inc. and Subsidiary participates in an employee benefit plan through its parent, Texas Bankers Association (the Association).

Defined Contribution Plan

The Association adopted a qualified retirement plan (401(k)) (the Plan) effective January 1, 1997, available to all employees who meet the service requirements specified in the Plan. Participating employees may contribute from 1% to 50% of their compensation to the Plan. The Plan consists of two components (1) Safe Harbor Match and (2) Profit-Sharing. With the Safe Harbor Match, the Association will match up to 4% of the employee's contribution if the employee contributes a minimum of 5% of their compensation. The Profit-Sharing component of the Plan was modified in January 2022. For employees hired after January 15, 2022, the Association will make a profit-sharing contribution equal to 3% of their compensation. Employees hired prior to January 2022 were grandfathered into the prior plan that included a contribution equal to 6% of the employees' compensation plus an additional 5.7% on compensation over the FICA wage level. The Profit-Sharing contributions made by the Association are partially vested with the employee after 2 years of service and fully vested after 6 years of service. Safe Harbor Match contributions made by the Association are 100% vested immediately. Contribution expense for The Bank Store, Inc. and Subsidiary was \$128,026 and \$104,100 for the years ending May 31, 2023 and 2022, respectively.

Note 7 - Contingent Liabilities and Uncertainties

Various legal claims arise from time to time in the normal course of business, which, in the opinion of management, will have no material effect on the Company's consolidated financial statements. The Company has no other commitments or off-balance sheet arrangements.



Privacy Policy

Privacy Policy

Effective Date March 21st, 2024

WWW.Compliancealliance.com is hosted by WPEngine in the cloud. This website is operated by Compliance Alliance, Inc. This policy serves as the policy regarding the collection, use and disclosure of personal, business data when you use our Service (s) and the choices you have with that data.

We use this data to provide and improve our services. By using any of our services, you agree to the collection and use of information in accordance with this policy.

Types of Data Collected:

While using any of our services we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you (“Personal Data”). Personally identifiable information may include, but not be limited to:

- Business email address
- First and last name
- Phone number
- Address, State, Zip code, City
- Cookies and Usage Data

We may use your personal business data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt out of receiving any, or all, of these communications from us by following the unsubscribe link or instructions provided in any email we send or by contacting us.

Usage Data:

We may also collect information on how you access and use the services (“Usage Data”). This usage data may include information such as your computer’s internet protocol address (e.g. IP address), browser type, browser version, the pages of our service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

Location Data:

We may use and store information about your location if you give us permission to do so (“Location Data”). We use this data to provide features of our services, to improve and customize our services.

You can enable or disable location services when you use our services at any time by way of your device settings.

Tracking Cookies Data:

We use cookies and similar tracking technologies to track the activity of our services and we hold certain information.

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Other tracking technology is used such as tags and scripts to collect and track information and to improve and analyze our services.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our services.

Some examples of cookies we use:

Session cookies: We use session cookies to operate our services.

Preference cookies: We use preference cookies to remember your preferences and various settings.

Security cookies: We use security cookies for security purposes.

Use of your Data:

We use the collected data for various purposes:

- To provide and maintain our services.
- To notify you about changes to our services
- To allow you to participate in interactive features of our services when you choose to do so
- To provide customer support
- To gather analysis or valuable information so that we can improve our services
- To monitor the usage of our services
- To detect, prevent and address technical issues
- To provide you with news, updates and general information about our services and events

Retention of Data:

We will retain your personal business data only for as long as necessary for the purposes set out in this Privacy Policy. We will retain and use this data to the extent necessary to comply with our legal obligations, resolve disputes and enforce our legal agreements and policies.

We will also retain Usage Data for internal analysis purposes. Usage data is generally retained for a shorter period of time, except when this data is used to strengthen the security of to improve the functionality of our services, or we are legally required to retain this data for longer periods.

Disclosure of Data:

Disclosure for Law Enforcement

Under certain circumstances we may be required to disclose your personal business data if required to do so by law or in response to valid requests by public authorities.

Legal requirements:

We may disclose your personal business data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend our rights or property
- To prevent or investigate possible wrongdoing in connection with the service
- To protect the personal safety of users of the service or the public
- To protect against legal liability

Security of Data:

The security of your data is important to us but remember that no method of transmission over the internet or method of electronic storage is 100% secure. While we strive to use the commercially acceptable means to protect your data, we cannot guarantee the absolute security of the data.

Service Providers:

We employ third party companies and individuals to facilitate our services, provide the service on our behalf, perform service related services to assist us in analyzing how our services are used.

These third parties have access to your personal business data only to perform those tasks on our behalf and are obligated to not disclose or use it for any other purpose.

Analytics:

We may use third-party service providers to monitor and analyze the use of our services.

Google Analytics:

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our services.

Payments:

We may provide paid products and/or services within the services. In that case, we use third-party services for payment processing (e.g. payment processors).

We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal business information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements ensure the secure handling of payment information.

Children's Privacy

Our services do not address anyone under the age of 18 ("Children").

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

Intended Purpose

All of our products, services, websites and emails are intended for business purposes only and are not intended for, or should be used for personal, family, or household purposes.

Changes to this Privacy Policy:

We may update our Privacy Policy Statement from time to time. We will notify you of any changes by posting the new Privacy Policy on our website, under Privacy Policy.

We will let you know via email and/or a prominent notice on our website, prior to the change(s) becoming effective.

You are advised to review this privacy policy statement periodically for any changes.



TBA Incident Response Plan



Incident Response Plan

The following procedures apply to both internal IT and managed service teams.

1. Isolate the affected user or device by revoking access to company resources:
 - Block sign-ins for impacted user
 - Reset password
 - Revoke active/MFA sessions
 - Block device-based access methods (VPN, conditional access, etc.)
 - Block mobile device access (BYOD/Corporate) via the following where applicable:
 - Conditional Access
 - MDM
 - MAM
 - If app passwords are present, delete existing app passwords
2. If internal IT handles incident, send notification to MSP and updated them on any changes. If MSP responds to incident, call and email client to notify and send updates on any changes.
3. Identify what services have been affected:
 - Inspect mailbox rules for any suspicious activity:
 - Auto-forwarding (internal/external)
 - Automatic deletions
 - Confirm with user via telephone validity of remaining rules
 - Perform virus scan of affected devices
 - Audit of logins and role assignments
 - Audit log of M365 changes
 - Verify vendor access if applicable
 - Export logs from all affected systems
4. Implement remediation:
 - Reset passwords
 - Restore backups if applicable
 - Start vendor support tickets if applicable
5. Perform a post-mortem, assigned to MSP
6. MSP to debrief client on post-mortem and present recommendations based on any findings



IT Disaster Recovery Plan

Policy Name: IT Disaster Recovery Plan

Organization: Texas Bankers Association (TBA)

Functional Area: Information Technology & Security

Regulation: None

Other Legal Requirements: None

| VERSION HISTORY | | | | |
|-----------------|--------------|---------------|---|--------------|
| VERSION | APPROVED BY | REVISION DATE | DESCRIPTION OF CHANGE | AUTHOR |
| 1.0 | Alvin Mills | 10/01/2020 | Multiple site changes from on-prem to cloud | Alvin Mills |
| 2.0 | Danny Garcia | 12/12/2023 | Personnel and MSP updates | Danny Garcia |

Texas Bankers Association (TBA) IT disaster recovery plan (DRP) is designed to ensure business continuity in the event of a disruptive event. Regular reviews and updates of this plan will be performed to adapt to changing threats and business needs. The goal is to ensure our plan meets or exceeds industry best practices and compliance standards.

1. Risk Assessment:

- Potential risks and threats to TBA operations with designated impact ratings

| Risk | Financial Impact | Operational Impact | Reputational Impact |
|-------------------|------------------|--------------------|---------------------|
| Natural disasters | High | Low | Low |
| Cyberattacks | High | High | High |
| Power outages | Low | Low | Low |
| Human errors | High | High | High |

2. Business Impact Analysis (BIA):

- Critical business functions and systems. Must be recovered quickly to minimize downtime and financial loss.

| Business Function | Critical | Recovery |
|--|----------|----------|
| Directory Services (All corporate workstations are joined to Microsoft Azure AD) | High | Med |
| Network Services (ISP, Network Management) | High | High |
| Communications (Exchange Online, Teams, SharePoint, Telecom) | High | High |
| iMIS Database (Main customer database hosted on ASI cloud) | High | High |
| Website (Texasbankers.com, BankersAlliance.com, ComplianceAlliance.com, etc.) | High | Med |
| Dynamics GP (Corporate Accounting system) | High | Med |
| Backup & Storage (Company SharePoint and OneDrive backup solution) | High | High |
| User Workstations (Corporate desktops, laptops, miscellaneous equipment) | Med | Med |

3. Disaster Recovery Team:

- Cross-functional disaster recovery team with clear roles and responsibilities.

- Director of information Technology – DRP coordinator (Primary)
- Director of Executive Operations – DRP coordinator (Secondary)
- Vice President of Marketing and Communications - Communications
- Managed Service Providers – Vendor/Partner liaison
- Chief Executive Officer – Status updates and communication relays
- Chief Operating Officer – Status updates and communication relays
- Chief Finance Officer – Status updates and communication relays
- General Counsel – Status updates and legal affairs
- President of Bankers Insurance Agency – Status updates and Insurance needs

4. Data Backup and Recovery:

- Regular back-up of all critical server data, including customer information, transaction records, and financial data is handled by the respective cloud service provider in accordance with our SLA. IT Department will work with each vendor to restore services and data. No physical servers or onsite storage are present in any TBA facilities.
- Workstation and user data is synced and backed up by OneDrive that is included with Microsoft Business Premium licensing. SharePoint and OneDrive cloud repositories are backed up via Datto Cloud Services. IT department will work with MSP to manage and restore any data necessary via the Datto cloud back up service in cases of cyber incidents or accidental deletion of important files or data.
- Testing of data recovery procedures is verified for effectiveness several times a year by service provider in accordance with SLA.

5. IT Infrastructure and Systems:

- IT infrastructure, hardware, software, and network configurations are inventoried, documented and managed by the IT Director. Some or all parts may be delegated to MSP in accordance with SLA.
- Plan for restoring or replacing hardware and software in case of damage, loss or theft is to follow IT Procurement Policy and register all systems in Microsoft Intune service for fast, easy deployment of corporate policy and user account setup including automated software installation and data synchronization via OneDrive sync services.
- Maintenance and patching of operating system and software inventories is handled by Microsoft Intune and managed by MSP in accordance with our SLA.

6. Communication Plan:

- The communication plan to inform employees, customers, and stakeholders about any disaster and recovery efforts is outlined below. Specific instructions will be provided for each scenario.
 - If email platform is available to internal staff, an urgent email message will be sent to all employees from our Disaster Recovery platform. Email will include as much detail as possible and estimated time of return to normal operations will be included.
 - If email platform is unavailable, an email will be sent to critical customers and vendor/partner with general incident information and direct them to website for updates.
 - Updates will be posted to the main TBA website with status of any major incidents directly on homepage.
 - If SharePoint is available, employees can view latest posted updates on main SharePoint site.
 - In cases of email unavailability, text messages will be sent via current telecom solution to all employees whose cell numbers are listed in the company phone directory.
 - In cases of email unavailability and in addition to text messages, we will send a company-wide voice message at the beginning of any major incident. Update messages will be sent every 2 hours after that for the first 48 business hours. After 48 hours, voice messages will be disseminated every 4 hours.

7. Alternate Worksite:

- In cases of major incident where access to the main work site is restricted or unavailable, employees will

be required to work remotely from home or other secure location.

- Employees are required to use corporate-owned devices to access any work-related systems. Home wireless networks must be secured with WPA PSK2 or stronger password.
- Employees may not use personal computer devices unless there has been explicit written permission by the Director of the IT department.

8. Vendor and Partner Relationships:

- Critical vendors/partners contact information is maintained in our iMIS system and designated distribution lists.
- Communication of disaster recovery plan will be shared with key vendors to ensure alignment and continuity.

9. Testing and Training:

- Regular DRP tests and simulations will be performed quarterly to ensure the plan's effectiveness. Schedule and detailed plans will be provided to DR team by Director of IT and Security. Reports on effectiveness will be generated and shared with team members in quarterly meetings.
- Ongoing training will be required of employees to keep up with their roles and responsibilities in the event of a disaster.

10. Documentation and Review:

- TBA shall keep all DRP documentation up to date, including contact lists, procedures, and recovery plans.
- Quarterly reviews and updates will be performed by the Director of IT annually or after any significant changes in business operations or technology.

11. Budget and Resources:

- Director of IT and CFO will allocate an appropriate annual budget and resources for disaster recovery efforts.
- Funds will be allocated for necessary services, equipment, training, and testing.

12. Compliance and Regulations:

- TBA will continuously seek information about relevant industry regulations and compliance requirements and ensure your DRP aligns with those regulations and requirements.

Summary of TBA Information Security Posture

Organization

Texas Bankers Association (TBA) information security is the responsibility of the IT Director reporting directly to the Chief Operations Officer. Responsibility for information security throughout the organization includes, but is not limited to, the development, maintenance, and enforcement of TBA's information security policy.

TBA partial outsources security to a third-party Managed Security Provider (MSP). The MSP monitors, scans, and assesses the computing environment 24x7 in accordance with the Service Level Agreement (SLA) stated in the contract. Known incidents and events are reported and escalated to the Director of IT for resolution. Results are remediated immediately when high and critical vulnerabilities are identified. TBA provides ongoing security awareness training, weekly cybersecurity newsletters and an Acceptable User Policy section included in the Information Security Policy of the employee handbook.

Environment

Texas Bankers Association provisions computer hardware and Microsoft 365 E5 Security licenses to all employees. These licenses provide cloud-based and desktop business applications. User accounts, systems, and endpoint devices are managed and controlled through Azure Active Directory Service and Intune Endpoint Management. Account administration and email services are handled by internal IT and the MSP. The network environment is managed, maintained and secured by the MSP, and consists of 24x7 monitoring of network switches, routers, firewalls, VPN services, and security appliances. TBA outsources various web sites to managed service providers such as ASI and WordPress.

IT Services provided by TBA:

- Security management and reporting
- Anti-virus
- Advanced Anti-malware protection
- Patch management
- Vulnerability scanning
- Security consultation
- Conditional access policies
- Network technical support
- User account activation and termination
- Phone services
- Email services
- Internet access services
- Domain registration and renewal
- Secure wireless networks
- Data backup and recovery services
- End point protection
- SOC as a service (outsourced)
- Technical support help-desk functions
- Consulting on IT best practices and security
- Website development and hosting
- Vulnerability scanning and resolution
- Inventory of hardware and software
- Licensing compliance assistance
- Purchases of IT equipment and software
- Security Awareness Training
- Incident response plan



TBA IT Security Posture - February 2024

Summary of TBA Information Security Posture

Organization

Texas Bankers Association (TBA) information security is the responsibility of the IT Director reporting directly to the Chief Operations Officer. Responsibility for information security throughout the organization includes, but is not limited to, the development, maintenance, and enforcement of TBA's information security policy.

TBA partial outsources security to a third-party Managed Security Provider (MSP). The MSP monitors, scans, and assesses the computing environment 24x7 in accordance with the Service Level Agreement (SLA) stated in the contract. Known incidents and events are reported and escalated to the Director of IT for resolution. Results are remediated immediately when high and critical vulnerabilities are identified. TBA provides ongoing security awareness training, weekly cybersecurity newsletters and an Acceptable User Policy section included in the Information Security Policy of the employee handbook.

Environment

Texas Bankers Association provisions computer hardware and Microsoft 365 E5 Security licenses to all employees. These licenses provide cloud-based and desktop business applications. User accounts, systems, and endpoint devices are managed and controlled through Azure Active Directory Service and Intune Endpoint Management. Account administration and email services are handled by internal IT and the MSP. The network environment is managed, maintained and secured by the MSP, and consists of 24x7 monitoring of network switches, routers, firewalls, VPN services, and security appliances. TBA outsources various web sites to managed service providers such as ASI and WordPress.

IT Services provided by TBA:

- Security management and reporting
- Anti-virus
- Advanced Anti-malware protection
- Patch management
- Vulnerability scanning
- Security consultation
- Conditional access policies
- Network technical support
- User account activation and termination
- Phone services
- Email services
- Internet access services
- Domain registration and renewal
- Secure wireless networks
- Data backup and recovery services
- End point protection
- SOC as a service (outsourced)
- Technical support help-desk functions
- Consulting on IT best practices and security
- Website development and hosting
- Vulnerability scanning and resolution
- Inventory of hardware and software
- Licensing compliance assistance
- Purchases of IT equipment and software
- Security Awareness Training
- Incident response plan

Overview

Total Prevented Incidents

5

Prevented Incidents Trend



Microsoft Identity Score

100%

The Identity Secure Score is a percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security.

Microsoft Secure Score

83.17%

1163.54/1399 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Multi-Factor Authentication

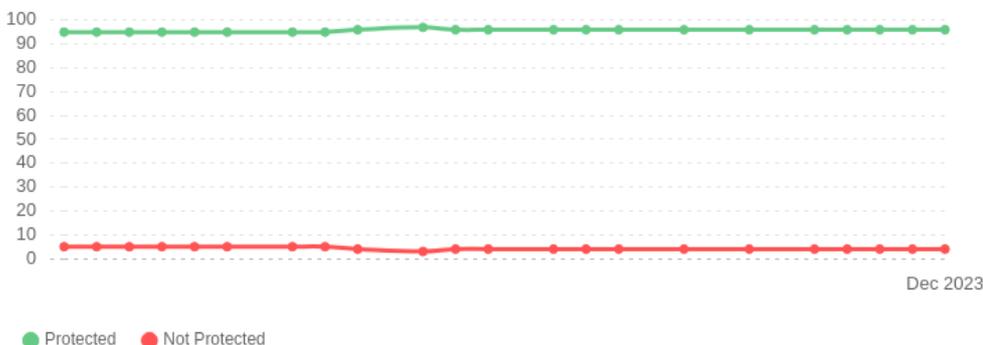
MFA Status

96%

Protected

4%

Not Protected



Prevented Incidents

Intercepted Risk Sign-ins Detections

5

Prevented Incidents

Sign-in Risk

A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

Top Risky Sign-in Accounts

| User | Count |
|------|-------|
|------|-------|

| | |
|-----------|---|
| null null | 4 |
|-----------|---|

Intercepted Risky Users Detections

No data available

User Risk

Risky activity can be detected for a user that isn't linked to a specific malicious sign-in but to the user itself.

Top Risky User Accounts

No data available

Intercepted Risky Countries

1

Intercepted Countries

Risky Countries

This is commonly used to block access from countries/regions where your organization knows traffic should not come from.

Top Risky Countries

| Country | Count |
|---------|-------|
|---------|-------|

| | |
|---|---|
|  US | 5 |
|---|---|

Intercepted Risky IPs

4

Intercepted IPs

Risky IPs

This is commonly used to block access from IPs where your organization knows traffic should not come from.

Top Risky IPs

| IP | Country | Count |
|----------------|--|-------|
| 185.189.25.242 |  US | 2 |
| 173.240.76.66 |  US | 1 |
| 185.189.25.231 |  US | 1 |
| 185.189.25.238 |  US | 1 |

Prevented Incidents

5

Total

5

Remediated

0

Recognized

41

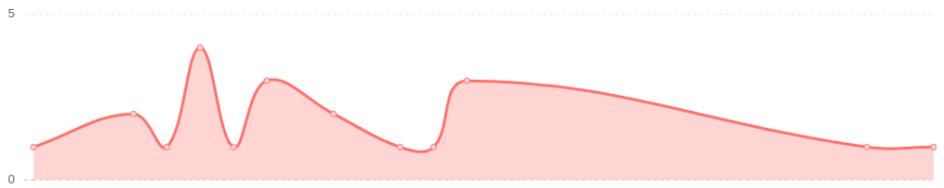
| Incident Type | User Impacted | Risk State | Location | Date |
|----------------------------|---------------------|-------------------------|----------|------------|
| signin: unfamiliarFeatures | null null | Remediated - Remediated | US | 2023-11-08 |
| signin: unfamiliarFeatures | null null | Remediated - Remediated | US | 2023-11-07 |
| signin: unfamiliarFeatures | null null | Remediated - Remediated | US | 2023-11-06 |
| signin: unfamiliarFeatures | null null | Remediated - Remediated | US | 2023-11-06 |
| signin: unlikelyTravel | undefined undefined | Remediated - Remediated | US | 2023-11-03 |

Overview

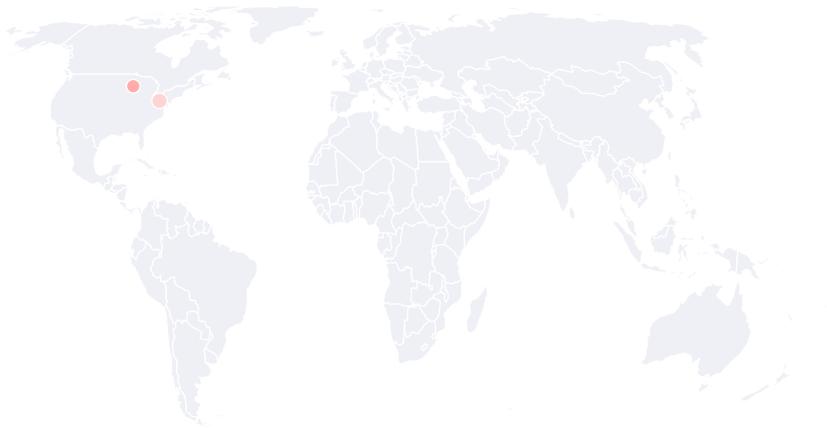
Total Risk Detections

21

Risk Detections Trend



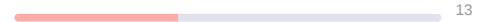
Location of Risk Detections



United States



Unknown



- High risk
- Medium risk
- Low risk
- Informational risk
- Unknown risk

Microsoft Identity Score

100%

The Identity Secure Score is a percentage that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security.

Microsoft Secure Score

83.17%

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

1163.54/1399 points achieved

Risk Detections

Top 5 Types of Risk Detections

| Risk Type | # of Detections |
|----------------------------------|-----------------|
| Reset user password | 6 |
| Unfamiliar Features | 4 |
| Atypical travel | 3 |
| Update Conditional Access Policy | 3 |
| Add conditional access policy | 2 |

Top 5 Accounts at Risk

| Account | Role | # of Detections |
|---------|--|-----------------|
| | Global Administrator | 8 |
| | Global Administrator Security Administrator | 3 |
| | Azure AD Joined Device Local Administrator | 1 |

Risk Detections

43

Monthly Security Summary

December 4, 2023 1:17:30 PM

Report is for the last 30 days: November 4, 2023 to December 4, 2023

Summary

...

A snapshot of your organization's protection state powered by Microsoft Defender for Endpoint. This report shows how well your organization is prepared to prevent and respond to cyberthreats.

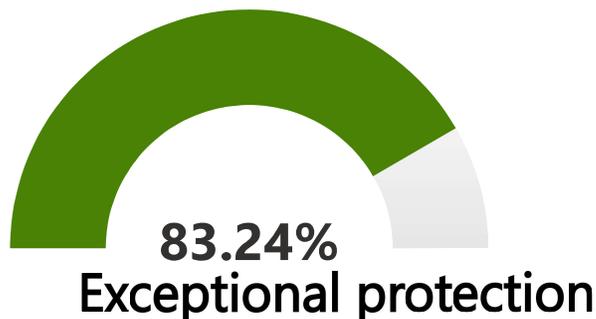
Your secure score is 83.24% and it improved by 0.61% from last month. It is 42.92% higher than other organizations of a similar size. 102 devices were onboarded this month. 0 URLs were blocked across 0 restricted categories.

Microsoft Secure Score

...

Your 83.24% secure score indicates that you have exceptional protection against threats

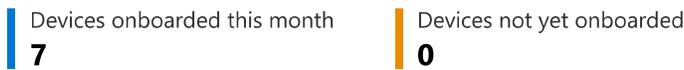
Your organization's overall cybersecurity strength has **improved by 0.61%** since last month. A higher number indicates more recommended actions have been taken, which minimizes your risk from attacks.



Your score is 42.92% higher than other organizations

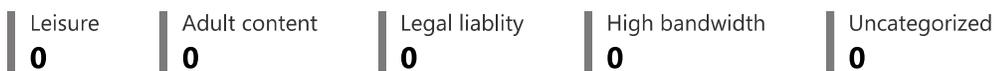


102 devices are onboarded



0 URLs blocked

User clicks blocked by category



MFA Report

Texas Bankers Association

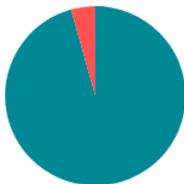
December 04, 2023

MFA Configuration

| Configuration Method | # of Employees |
|--------------------------|----------------|
| Conditional Access | 88 |
| Per-User MFA | 2 |
| Security Defaults | 0 |
| Duo & Conditional Access | 0 |

MFA Status

| | |
|---------------|----|
| Protected | 88 |
| Not Protected | 4 |



Authentication Methods

| | |
|--------------------|-----|
| Authentication App | 40 |
| Phone/SMS | 84 |
| Security Key | 0 |
| Other | 177 |





TBA IT Security Policy

| | |
|----------------------------------|--|
| Policy Name: | Information Security Policy |
| Organization: | Texas Bankers Association (TBA) |
| Functional Area: | Information Technology & Security |
| Regulation: | None |
| Other Legal Requirements: | None |

PURPOSE & OBJECTIVES

This policy statement has been established to communicate TBA’s position on Information Security.

This Information Security policy establishes the responsibilities of users of TBA’s information systems, including employees, affiliates, contractors, and any other authorized users, for protecting the TBA’s non-public information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. As used in this Policy, the term, “Information Security” refers to the general practice of protecting TBA’s non-public information and information systems and encompasses the more specific terms, that are often used to refer to particular aspects of the security of electronic data and computer systems, such as, “cybersecurity,” “network security,” “mobile security,” “Internet security,” or “computer security”. These sub-categories of Information Security are interrelated and share the common goal of protecting the confidentiality, integrity, and availability of non- public information, which is the objective of this Policy. TBA leadership understands the importance of Information Security to TBA’s business, and that the manner in which information is handled by TBA reflects TBA’s commitment to maintain Information Security.

OPERATING PARAMETERS

Information Security Standards:

TBA shall establish Information Security Standards, which outline TBA’s Information Security objectives. TBA shall maintain an Information Security Program led by the VP IT & Security that supports the Information Security Standards and this Policy. The Information Security Standards will include provisions for an assessment of TBA’s cyber security risk and preparedness taking into consideration relevant guidance from FFIEC.

USER RESPONSIBILITIES

Technology and Information Assets:

All users of TBA systems, including all directors, employees, affiliates, contractors, and any other authorized users are obligated to protect the technology and information system assets of TBA from unauthorized access, theft and destruction. The technology and information system assets are made up of the following components:

Computer hardware: Includes all laptops, desktops, printers, scanners, monitors, copiers, any miscellaneous peripherals used to conduct company business.

System Software: Includes, but not limited to, operating systems, email clients, cloud applications, word processing, spreadsheets, database management systems, backup and restore software,

Application Software: Any software used by the various departments within TBA. This includes custom written software applications, and commercial off the shelf packages.

Communications: Network hardware and software including routers, hubs, switches, firewalls, and associated network management software and tools and communication applications such as VPN clients.

Protection of Non-public Information:

TBA employees are personally responsible for protecting all non-public information used and/or stored with their accounts on TBA's information systems. This responsibility includes protecting the user's account logon IDs, passwords and locking systems when the user is not actively present. Furthermore, users are prohibited from making unauthorized copies of such non-public information and/or distributing it to unauthorized persons outside of TBA. TBA's Data Privacy Policy and Data Privacy Standards shall establish additional user requirements with respect to security and the protection of non-public information.

Acceptable Use:

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to TBA systems for which they do not have authorization. TBA's employee handbook shall establish additional user requirements with respect to acceptable use.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the Director of IT. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in TBA's computer security, any incidents of misuse or violation of this Policy to their immediate supervisor and/or the company helpdesk.

Users are required to complete security awareness training annually. In addition, users are enrolled in email campaigns aimed at cyber awareness and general education about current threats.

Use of the Internet:

TBA will provide Internet access to users who are connected to the internal network and who have a business need for this access.

The Internet is a business tool for TBA. It is to be used for business-related purposes such as: communicating via electronic mail with business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature or any other purpose which is illegal or for personal gain.

The TBA's employee handbook shall establish additional user requirements with respect to internet use.

AUTHORITIES DELEGATED TO MANAGEMENT

The authority for the implementation of this policy is delegated to the Chief Executive Officer (CEO) or his/her designee.

AUTHORITIES FOR APPROVAL AND MANAGEMENT

The CEO oversees final approval of this policy and any future policy changes. The authority for implementation of this policy is delegated to the CEO's designee.

PROCESS FOR ADDRESSING EXCEPTIONS

Exceptions to this policy may be approved by the CEO or their designee.

REPORTING REQUIREMENTS

The CEO expects their designee to report on any issues arising under this policy requiring CEO attention or action. The CEO's designee shall report to the CEO on their assessment of the effectiveness of the Information Security policy at least annually.

SANCTIONS

TBA will take appropriate disciplinary action for any violations of this policy, up to and including termination of employment and/or civil or criminal prosecution.



TBA Security Controls

TEXAS BANKERS ASSOCIATION CYBERSECURITY MEASURES

1 ENDPOINTS

1. All endpoints are covered by Microsoft Defender for Endpoint P2. Features include:
 - a. Next-generation antimalware
 - b. Endpoint firewall
 - c. Web control / category-based URL blocking
 - d. Device-based conditional access
 - e. Controlled folder access
 - f. Endpoint detection and response
 - g. Automated investigation and remediation
 - h. Cyberthreat and vulnerability management
 - i. Threat intelligence
 - j. Sandboxing
2. Endpoints are enrolled in Intune for mobile device management which allows for:
 - a. Enforcing security baselines
 - b. Asset management
 - c. Application management

2 NETWORK

1. Protection at the Network level provided by Meraki Advanced Security which features include:
 - a. Advanced Malware Protection (AMP) with Cisco Threat Grid
 - b. Content filtering
 - c. Intrusion detection and prevention (IDS/IPS)
 - d. Geofencing
 - e. Web search filtering

3 WEB

1. Filtering, management, and protection at the network level via Meraki
2. Filtering, management, and protection at the device level via Microsoft Defender for Endpoint P2
3. Filtering, management, and protection across devices both within and outside of the network leveraging Microsoft Defender for Cloud Apps. Features include:
 - a. Cloud App Discovery
 - b. Cloud access security broker
 - c. Conditional Access App Control

- d. Cloud App risk assessment
- e. Cloud App Authorization
- f. Anomaly detection and behavioral analytics
- g. Security baselines enforcement

4 EMAIL

1. Email security software used is Microsoft Defender for 365 P2 which features include:
 - a. Phishing training and testing
 - b. Automated investigation and remediation
 - c. Cyberthreat and vulnerability management
 - d. Threat intelligence
 - e. IP and DNS filtering and protection
 - f. Sandboxing
 - g. Attachment scanning
 - h. Uses SPF, DMARC, and DKIM for email security against spoofing and phishing Identity
 - i. MFA
 - j. External emails are tagged

5 BACKUPS

1. Backups of OneDrive, exchange, calendars, and SharePoint are provided by Datto SaaS Protection whose features include
 - a. 9 georedundant datacenters
 - b. 3X daily cadence
 - c. Immutable backups
 - d. Encryption
 - e. MFA protection

6 PATCHING

1. Workstations drivers and OS patched via Intune
2. Applications patched via Ninite

7 IDENTITY

1. Leverages Microsoft Defender suite and Intune for identity management
 - a. Geoblocking at the cloud and email level
 - b. Atypical travel and risky sign ons monitored at cloud and email level
 - c. Machine learning and AI flags atypical behaviour

8 VULNERABILITY MANAGEMENT

1. Leverages Microsoft Defender suite to address vulnerabilities and reduces attack threat landscape
 - a. Microsoft provides specific recommendations based on
 - i. Security Standards and Best Practices
 - ii. Threat Intelligence
 - iii. Behavior analytics
 - iv. Incident Response Data
 - v. Machine learning and AI
 - vi. Community Feedback
 - b. Microsoft assesses the environment for risks based on
 - i. Existing security controls
 - ii. Existing security configurations
 - iii. Industry best practices
 - iv. User and device behavior
 - v. Threat intelligence
 - c. Microsoft measures drift from security controls and baselines
 - d. Microsoft prioritizes recommendations based on criticality
 - e. TBA's secure score (82.25%) is more than double the average for companies of a similar size (40.25%)
2. Leverages Microsoft controls to give least privilege and just in time access
3. Leverages MSP cybersecurity team to reduce attack vectors and investigate potential security events
 - a. The team consists of 6 members
 - b. 24/7/365 alerting is configured
 - c. Regular hours of operation are 7am to 6pm, M-F



TBA IT BYOD Policy

| | |
|----------------------------------|--|
| Policy Name: | Bring Your Own Device Policy |
| Organization: | Texas Bankers Association (TBA) |
| Functional Area: | Information Technology & Security |
| Regulation: | None |
| Other Legal Requirements: | None |

PURPOSE & OBJECTIVES

This policy is intended to include all employees who use personally-owned computing devices on the TBA network and/or accesses resources, cloud services, or applications owned and managed by TBA.

In reference to this policy, personally-owned devices can include, but are not limited to: desktop computers, laptop computers, tablet computers, smartphones, external or mobile storage devices, and any other device capable of storing, processing, and/or transmitting data, wired, wireless, or cellular.

Policy

It is the policy of TBA that personally-owned devices may be used in the performance of TBA-related work and services with the express approval of the owner's department head and Director of IT. Devices must comply and operate within the constraints of proper operational security. This will be approved so long as the actions taken by personnel, the use of the devices, and the devices themselves do not pose a threat to TBA, its personnel, its resources or any of its partners.

Sensitive or confidential information shall not be downloaded or stored on personally owned devices, including mobile storage devices. Any device that is used for TBA- related work must also meet the same requirements as dictated by Information Technology operations and must comply with all applicable TBA security policies.

To this end –

Devices MUST:

- be encrypted
- be registered with the Microsoft Intune mobile device management service
- meet TBA security service requirements

Users MUST:

- sign the information security policy
- take all actions necessary to protect the device from loss, theft, or information disclosure
- notify TBA immediately upon loss, theft, or suspicion of disclosure
- work with TBA to ensure all TBA related data is removed from the device before disposing of, trading, upgrading, selling, or otherwise replacing the device or terminating from TBA

All TBA -related data created on, stored on, processed by, or transmitted to or from the device is the property of TBA. It is the responsibility of the device owner to properly protect that data, and due care must be shown in the protection of the device and its data.



Cyber Hygiene Report February 2024

Please click the title to access the report



Citrix Soc 2 Report

This report is attached separately due to it being a third-party company and report. We do not have permission to attach the SOC 2 report to our company documentation.

Citrix Systems is the whole owner of ShareFile. ShareFile is used on occasion by our Review Alliance teams to share files.



Microsoft 365 Assessment

Microsoft 365 Assessment

Texas Bankers Association

As of January 18, 2024



Table of Contents

1 Introduction.....3

1 Introduction

Task

CoNetrix was contracted to perform a Microsoft 365 Assessment, defined in signed quote number 94482-00-2. Information collection and inspection was completed as of the date on this summary.

Objectives

The primary objective of this assessment was to perform a review of the association's Microsoft 365 environment. The individual findings documented in the report include recommendations that will assist the association in providing necessary internal control improvements.

The association's management is responsible for establishing and maintaining adequate IT processes, controls, and supporting infrastructure. Internal controls are designed to provide management with sufficient assurance that assets are protected from unauthorized access or use, and that regulatory compliance is maintained as services are provided.

Scope

CoNetrix based this engagement on the latest Federal Financial Institutions Examination Council's (FFIEC) Information Technology Work Programs, which we expanded in key areas particularly relating to Information Technology infrastructure and security best practices.

The scope of this engagement aligns with a number of industry standards, including:

- NIST Cybersecurity Framework
- NIST Special Publications
- FFIEC regulations and guidance
- Microsoft security recommendations
- CIS Microsoft 365 Benchmark 1.5
- CIS Microsoft 365 Benchmark 2.0

The engagement is performed in accordance with the ISACA Standards and Guidelines for IS Audit and Assurance.



Executive Summary

General Notes

The final report is based upon an evaluation of applicable controls in place as of the date on the report. Any projection of these conclusions into the future may be inaccurate due to internal or external changes that may have taken place.

The report details all current engagement findings. The associated work program document defines the full scope of the engagement including risk levels previously accepted by the association and areas in which no deficiencies were noted.

The intent of the report is to aid understanding of each issue, identify severity of the vulnerabilities, analyze potential impact of remediation, and offer possible solutions to mitigate information security risks.

Association staff cooperated fully in the provision of requested materials, which is indicative of the high level of competence observed within the association's Information Technology management. Access to the association's IT resources (equipment and personnel) was also provided as needed. Furthermore, as items were discussed during the assessment process, the association showed the willingness and ability to respond in a timely fashion to resolve issues. A number of finding elements were reported by the association to be resolved prior to the delivery of the final report.



A trusted partner for banks of all sizes
with the resources to make a difference
– every day and every week.

[Compliancealliance.com](https://www.compliancealliance.com)