Internal Audit

Audit Report

March 29, 2023

TO: Alanna Williams
BSA Officer

Tim Ayala
Chief Risk Officer

AUDIT ENTITY: BSA

2023 AUDIT PLAN INHERENT RISK ASSESSMENT: High

Cc: Lisa Burkhart, BSA Manager
Teresa Clanton, BSA Manager
Nora Klein, BSA Manager
Valerie Partlow, BSA Manager

Contents

Audit Report

Engagement Overview

The Internal Audit Department of Pinnacle Financial Partners, Inc. and Pinnacle Bank ("PNFP", "Pinnacle", the "Bank" or "the Company") performed an independent audit of the Company's Bank Secrecy Act (BSA) function, which is a centralized, second line of defense function responsible for managing risks related to money laundering and financial crimes.

The department is led by BSA Officer Alanna Williams, who reports to the Bank's Chief Risk Officer. Alanna is supported by four BSA managers who oversee Alerts, High Risk Monitoring, Quality Control and Currency Transaction Reports (CTRs). In total, the BSA team includes 36 associates.

The primary objective of the BSA Department is to monitor the Bank's client base for instances of potential money laundering and financial crimes and to report suspected illegal activity to law enforcement.

Engagement Objective and Scope

The objective of this audit was to independently evaluate the design and effectiveness of the Company's Bank Secrecy Act (BSA)/Anti-Money Laundering (AML)/Office of Foreign Assets Control (OFAC) Program (the "Program") and its processes and key controls established to ensure compliance with applicable laws and regulations. The Bank Secrecy Act of 1970 (BSA) is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. BSA requires U.S. financial institutions to assist U.S. government agencies in detecting and preventing financial crime.

The period reviewed covered 12 months from January 1, 2022 to December 31, 2022. The duration of this audit was approximately eight weeks and commenced on January 17, 2023.

The methodology used to determine our scope of review was based on an assessment of the required elements, referred to as pillars of a BSA/AML/OFAC Compliance program as defined by the Federal Financial Institutions Examination Council (FFIEC):

- Pillar 1 – System of internal controls: includes the bank's policies, procedures, and processes designed to limit and control risks and to achieve compliance with BSA/AML/OFAC requirements;
- Pillar 2 – Designated BSA Officer: the board of directors must designate a qualified individual to serve as the BSA/AML/OFAC Officer who is responsible for coordinating and monitoring day-to-day BSA/AML/OFAC compliance;
- Pillar 3 – Employee Training Program: The Bank must ensure that its personnel receive general and role-specific training in applicable aspects of BSA/AML/OFAC;
- Pillar 4 – Independent Testing: The Program must be independently tested (audited) by the internal audit department, outside auditors, consultants, or other qualified independent parties, with a frequency commensurate with the BSA/AML/OFAC risk profile of the bank;

- Pillar 5 – Customer Due Diligence / Beneficial Ownership: New Customer Due Diligence Requirements for Financial Institutions went into effect on May 11, 2018, requiring covered financial institutions to identify and verify the identity of beneficial owners of a legal entity at the time the legal entity opens a new account, as well as develop risk profiles and conduct ongoing monitoring of applicable beneficial owners.

New products and services risk management and vendor oversight were out of scope as they fall under other audit entities or will be covered in future audits.

Methodology

Internal Audit begins the audit process by evaluating the risk environment and identifying the key risks associated with each audit entity. This analysis incorporates management's identified risks and controls as well as risks that have not yet previously been formally documented by management. Then, the engagement team designed procedures to test the documented controls based on the discussions with management, walkthroughs of the relevant systems/applications and review of the processes and controls for the areas in scope.

Summary of Issues and Key Themes

We reviewed the processes performed by BSA to evaluate documentation, control design and effectiveness and policy adherence. Based on our procedures performed, we have noted areas where further improvements are needed to strengthen the overall control environment for BSA. Specifically, we noted issues related to the following:

Issue Identified	Rating	Root Cause
BSA Program Process Inefficiencies	High	Technology – Design
Remote Deposit Capture (RDC) Client Reviews	Medium	People – Understanding & Accountability
Enhanced Due Diligence (EDD) Reviews	Medium	Process – Manual Process
Annual Risk Assessment Data Collection	Medium	People - Competency
Annual Review of Brokered Deposits	Low	People – Understanding & Accountability
New Account Anticipated Activity Reviews	Low	Process – Manual Process
Accuracy / Completion of Office Information on CTRs	Low	People – Understanding & Accountability
Annual BSA Training Completion	Low	Governance - Culture

The most significant issues noted within the report align to the following themes:

- System limitations within Patriot Officer have created inefficiencies both in the department's work load in the number of false positive alerts requiring evaluation and the need for manual processes to compensate for the system limitations; and
- Given the system limitations noted above, the use of manual processes presents a high risk of human error as it relates to day-to-day execution. Manual processes require high levels of judgement and institutional knowledge to ensure accuracy of inputs and outputs.

Management Response

Management agreed with the risk and related issues identified above and has developed sufficient and appropriate action plans to further improve the audit entity's risk management framework.

Audit Conclusions and Rating

While the above audit issues were identified, Internal Audit did not identify any indication of systemic non-compliance with the BSA. The BSA team accomplishes a meaningful amount of work with great diligence. The team undertakes their work systematically and methodically to mitigate the risks associated with money laundering, terrorist financing and other illicit financial activity. While a number of issues were identified, the majority of issues can be tied to inefficiencies of the suspicious activity monitoring system, Patriot Officer, and the manual processes implemented to compensate for the system's current design. As a result, management should ensure current processes and controls are effectively mitigating risk.

Management has started the process of evaluating a replacement tool more appropriate for the Bank's current size and complexity; however, full implementation is not likely to occur until late 2024. It is the opinion of Internal Audit that the BSA function would greatly benefit from the identification of a dedicated associate tasked with operational and process oversight duties, such as system reconciliations and report production, to aid in work completion and accuracy. Such an addition to the BSA function will be invaluable as management continues the process of system conversion given the current staffing constraints.

When reviewing the totality of audit evidence obtained during the execution of this audit which was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*, we believe risk has been managed at a generally acceptable level although management should enhance control activities to avoid adverse operational impact, reputation damage, and/or financial loss and has resulted in an overall Audit Entity Report Rating noted as Satisfactory with Recommendations, as defined in Appendix II.

Dana Sanders
Chief Audit Executive

Erin Demarco
Auditor-In-Charge

Appendix I: Audit Issues and Management Action Plans

AUDIT ISSUE		
2023 BSA A1	BSA Program Process Inefficiencies	**Rating**: High

Background: The BSA team leverages the Patriot Officer software platform to scan activity, trigger alerts, etc. Patriot Officer was implemented in 2006 to aid in suspicious activity monitoring when the bank was less than $2 billion in assets. Since that time, the bank has experienced significant growth both organically and through merger and acquisition activity increasing the complexity and volume of transaction subject to review. As such, the usefulness of Patriot Officer's functionality has diminished over time increasing the need for supplemental manual monitoring processes. Given the volume of activity, manual processes create work load issues and present risks related to inefficiency and human errors. During the course of 2022, the BSA team evaluated more than 74,000 rule triggers, which produced more than 23,000 suspicious activity alerts. Alerts generated resulted in only 723 SARs filed representing a realization rate of approximately 3 percent. The current system produces an excessive number of false positive alerts that are each required to be manually reviewed, researched, and documented prior to closure, even when no suspicious activity is present.

Additionally, the Patriot Officer system offers limited capabilities and functionality in terms of automation and efficiency in other critical areas such as high-risk customer management, CTRs and CTR Exemptions, and SAR 90-day follow-up management. As such, manual work around solutions have been implemented over time in an attempt to manage the ever-growing workload.

Issue: Through detailed transactions testing conducted in accordance with FFIEC examination procedures, Internal audit identified the following errors and exceptions:

- Suspicious activity alerts were not researched and dispositioned timely;
- In one instance, a SAR 90-day follow-up review was not completed;
- CTR Exempted clients were ineffectively managed resulting in missing CTRs and a missing annual review;

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties.

Root Cause: Root Cause: Technology – Integration or Obsolescence: System limitations are creating inefficiencies related to work load and require manual work around solutions, which are prone to human error.

Recommendation: As it relates to past-due alerts and missing requirements such as 90-day follow-up reviews, SARs, and CTRs, we recommend the following:

- Management should complete a review of all related account activity, determine if a SAR or CTR filing is warranted, and file, if necessary.
- Management should also perform a reconciliations and lookbacks of the 2021 and 2022 manual populations to system generated populations as appropriate to determine if any additional filing or review requirements were missed.

On a go-forward basis, management should consider the following:

- Management should consider the addition of a dedicated associate tasked with operational and process oversight duties such as system reconciliations and report production to aid in work completion and accuracy;
- Management should partner with PNFP Quantitative Analysts to assess the tuning of rules and alerts data sets to identify potential areas for enhancement;
- Given system limitations, management should prioritize more complex activity and relationships so research is completed timely, and any suspicious activity is reported timely to law enforcement;
- Implement routine reconciliation between the Bank's BSA/AML monitoring software, Patriot Officer, and working lists maintained outside of Patriot Officer;
- Explore ways to streamline the alert management and 90-day review process, including possible functionality within the current system; and
- Develop a process change management checklist to ensure that process enhancements are carefully executed and modifications do not result in unintended consequences.

Management Action Plan:

Alerts

AML Management implemented a new tracking mechanism outside of PO for Escalated Alerts, SAR filings, SAIF Referrals and Subpoenas, and 90 Day SAR Reviews in January of 2022. This is an access database with the ability to pull reports on any outstanding case types both by type and in total. During the audit review, there were instances in which a 90-day review was missed, and a SAR investigation was not filed timely. Management will research other avenues for case management, reconciliation, and gap analysis to include systems and/or processes currently being used for tracking. This will include partnering with IT System Support analyst and PO liaison to identify and test any features that may be available currently within PO that could aid and assist with validation and tracking of AML investigation types. If available within PO, management will consider and test before implementing any new functionality.

AML Management/Team will complete a review for any past due items of all related account activity to determine if a SAR is warranted, and file, if necessary.

CTRs

A comparison of the annual CTR exemption spreadsheet with a list from Patriot Officer has been completed prior to completing the audit review. Any necessary changes were made when a difference was found. This will become a quarterly process when the annual quarterly review is completed. A reconciliation was completed that included a review of exemption revocations to ensure any missed CTRs were identified and filed. A review of first quarter annual reviews has been completed to be sure Patriot Officer and Work with Exemptions (JH) is correct and updated. Additional items have been added to the CTR Exemption and CTR Annual Exemption Review checklists to prevent any discrepancies. Procedures will be revised to include a check and balance/reconciliation of Patriot Officer and the manual exemption spreadsheet.

BSA Management will evaluate and consider adding qualified analyst that can take the role of a Program Manager to validate system reconciliations, reports production to ensure validation and accuracy is being performed. In addition, a lookback of the 2021 and 2022 data both in Patriot Officer

and outside of PO will be reconciled and any outstanding or potentially missed investigations will be completed if identified.

Issue Owner(s): Nora Klein
Issue Due Date: 12/31/2023

AUDIT ISSUE		
2023 BSA A2	Remote Deposit Capture (RDC) Client Reviews	**Rating**: Medium

Background: RDC allows a client to deposit certain forms of non-cash negotiable instruments using a scanner provided by the Bank. RDC may expose banks to various risks, including money laundering, fraud, and information security, and is only available to a select group of clients that meet certain criteria. Additionally, Banks face challenges in controlling the location of RDC equipment, because the equipment can be readily transported from one jurisdiction to another. This challenge is increased as foreign correspondents and foreign money services businesses are increasingly using RDC services.

RDC clients are deemed to be higher-risk and the Bank has established procedures for monitoring RDC clients more closely due to the level of risk associated with this client type. The BSA Department monitors high risk RDC clients quarterly based on a list of criteria established to target the clients with the highest risk.

Issue: Testing of the RDC review process revealed the following:

- Multiple RDC reviews that were not performed as required by policy. This was due to two separate issues:
    - At least 49 high-risk RDC client reviews were inadvertently missed during the course of 2022 due to incorrect application of filtering criteria in excel; and
    - Inaccurate reporting during the year may have led to additional missed reviews. Due to reporting inaccuracies, IA was unable to perform completeness testing over the full population of RDC clients.
- Due to a reporting issue with a third-party vendor, IA confirmed IP address verifications were not completed for any RDC reviews performed in 2022. However, it was noted on the Client Review forms that a review of IP addresses had been completed.
- One instance where a review of negative news was not completed, as required by procedures.

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: Technology – Integration or Obsolescence: Systems containing RDC client and activity data is not integrated across the organization requiring a highly manual process for aggregation, which led to data quality issues. Additionally, misunderstandings in the application of filtering criteria led Management to make misinformed risk based decisions related to RDC reviews.

Recommendation: We recommend management develop and implement an enhanced tracking mechanism to identify and track required RDC reviews. Additionally, management should consider partnering with the Treasury Management Department to develop appropriate RDC risk mitigation

procedures that define 1st and 2nd line of defense roles and responsibilities. Procedures should contemplate RDC risk mitigation factors as defined by the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual.

We also recommend management perform a lookback to determine which RDC reviews were missed and perform such reviews accordingly. In addition, when third-party reports are determined to be inaccurate, we recommend completing reviews once the data has been corrected and that management work with TPRM to evaluate vendor performance. We recommend management follow up with the third-party vendor to address the IP Address reports needed. In addition, we recommend negative reviews be completed for all RDC client reviews, as required by policy.

Management Action Plan:
BSA-Risk has completed a lookback to identify missed RDC reviews for 2022. There was a total of 95 identified in 2022. There was 1 RDC client reviewed in 1Q2022 and 3 in 4Q2022. In addition, the lookback identified a RDC client with two Customer IDs. There were 51 clients from 2022 lookback that met criteria to be reviewed in 1Q2023. The remaining 40 clients from 2022 lookback were added to the 1Q2023 review list. The decision was made to conduct current reviews based on last quarter's activity to identified current activity trends rather than older activity. If suspicious activity was identified, it would be referred to AML group for further lookback.

As of 2/9/2023 an email from IT-Systems Support, Jack Henry engineers were waiting on logs to upload the Reports. Once reports were loaded this should catch up reports until automation can be resumed.

BSA-Risk will put quality control measures in place to ensure the prior week's RDC IP daily reports were reviewed, and documentation was noted on the RDC IP working log. The quality control will be a lookback of previous week's RDC IP daily reports, and the working log has been updated appropriately.

Requested from IT-Systems Supports to provide any applicable quality controls measures to ensure reports are being automatically uploaded appropriately to Goldleaf.

Issue Owner(s): Teresa Clanton
Issue Due Date: 12/31/2023

AUDIT ISSUE		
2023 BSA A3	Enhanced Due Diligence (EDD) Reviews	**Rating**: Medium

Background: Customers that pose higher money laundering or terrorist financing risks, (i.e., higher risk profile customers), present increased risk exposure to banks. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk is referred to as enhanced due diligence (EDD).

The bank performs EDD reviews after account opening for clients identified as higher risk. EDD procedures have been established for a variety of high-risk client types such as cash intensive, wire

intensive, Money Service Businesses(MSBs)/MSB Agents, Non-Resident Aliens, Owner-Operated ATMs, Third-Party Payment Processors, Industrial Hemp Cultivators/Producers, etc. At the time of EDD review, if warranted, due diligence documents are requested and appropriate documentation is returned to BSA by the Financial Advisor. Review notes are added to Patriot Officer and any risk rating changes are made within the core system.

Issue: The following procedural exceptions were noted when testing a sample of thirty-two EDD reviews:

- One instance where required licensure and crop inspection documentation was not obtained for a hemp producer client;
- Two instances where required registrations, licenses, ATM agreements, and/or MSB Acknowledgment documentation was not obtained for MSB and MSB Agent clients;
- One instance where the high-risk team identified a client acting as an MSB through review of check cashing activity but did not timely escalate the activity to the SAR team; and
- Two instances where EDD code updates within Patriot Officer were not consistent with EDD review comments.

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: Process – Manual Process: The process of obtaining appropriate due diligence documents is highly manual in nature, requires a high-degree of judgement and knowledge to determine appropriate documentation, and involves multiple handoffs between the first and second lines of defense.

Recommendation: We recommend management consider centralizing the document and information gathering process using a ticketing and exception system such a ServiceNow to increase efficiency.

Alternatively, Empowering the BSA Department to reach out to the client directly via phone and/or letter, will not only make the process more efficient, but would allow those with specialized knowledge to be the primary point of contact.

Management Action Plan:
BSA Risk has reached out to IT-ServiceNow to discuss how ticketing and exception systems is utilized for monitoring outstanding request as well as becoming a centralized documentation system.
In the case that ServiceNow will not offer a viable solution, Management will reevaluate this action plan and determine the best course of action.

Issue Owner(s): Teresa Clanton
Issue Due Date: 12/31/2023

AUDIT ISSUE		
2023 BSA A4	Annual Risk Assessment Data Collection	**Rating**: Medium

Background: While not a specific legal requirement, a well-developed BSA/AML risk assessment assists the bank in identifying risk events such as potential money laundering, terrorist financing and other illicit financial activities, and in developing appropriate internal controls. Understanding the risk profile enables the bank to better apply appropriate risk management processes to the BSA/AML compliance program to mitigate and manage risk and comply with BSA regulatory requirements. The BSA/AML risk assessment process also enables the bank to better identify and mitigate any gaps in controls. The BSA/AML risk assessment should provide a comprehensive analysis of the bank's money laundering, terrorist financing, and other illicit financial activity risks.

Issue: Through testing procedures performed over the risk assessment, we noted the following discrepancies:

- The risk assessment does not contemplate the bank's private banking operations. Private wealth banking is offered in certain lines of business throughout the bank;
- The risk assessment only contemplated timed brokered deposits and did not include demand brokered deposits; and
- The listing of bank subsidiaries included in the risk assessment was incomplete. Additionally, the assessment of BSA/AML scope applicability was inaccurate for one subsidiary (PNFP Capital Markets)

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: People – Competency: The process of obtaining complete and accurate data for the annual risk assessment requires a high degree of judgement and institutional knowledge. Current practices do not contemplate new and expanding services and business lines or verification of data accuracy and completeness.

Recommendation: We recommend management review and challenge the current risk assessment process to ensure data contained within the risk assessment is complete and accurate and considers new products and services. Management should consider vetting the risk assessment with other members of the second line of defense team and other leaders to verify the information utilized is complete and accurate. Management should fully document the risk assessment data collection process including all sources of data obtained.

Management Action Plan:
Existing practices will be reviewed, documented at the time of the next risk assessment review beginning in June 2023. Management will fully document the risk assessment data collection process to include who the information was collected from, where the source obtained the data (either by BSA or if from another line of business). Furthermore, Management will vet the risk assessment data with other members of the second line of defense team and other leaders thus ensuring the information collected is complete and accurate.

Issue Owner(s): Alanna Williams
Issue Due Date: 09/30/2023

AUDIT ISSUE		
2023 BSA A5	Annual Review of Brokered Deposits	**Rating**: Low

Background:
Pinnacle may purchase brokered deposits from time to time to supplement liquidity. Brokered deposits represent a range of clients and could include clients at a higher risk for money laundering and terrorist financing activities.

Accordingly, brokered deposits are considered higher risk as regulatory oversight and BSA/AML applicability varies from broker-to-broker and each broker operates under its own guidelines. However, all brokers are subject to OFAC requirements which includes customer due diligence and OFAC screening.

The BSA team conducts an annual review of all brokered deposits on core to assess the adequacy of the bank's systems to manage the associated risk.

Issue: Testing of the 2022 annual review of brokered deposits revealed that the review included brokered demand deposits only and did not include timed brokered deposits.
Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: People – Understanding & Accountability: Data related to Brokered Deposits was not obtained from the proper source resulting in incomplete data collection.

Recommendation: Management should work with the BSA associates to ensure that all associates understand the rationale behind the task at hand to ensure that the associated risk is being appropriately mitigated. To the extent possible, management should consider revising procedures to include the rationale for a process and to ensure data is obtained from a reliable source to ensure the information received is complete and accurate.

In regards to the annual brokered deposit review, at a minimum we recommend management partner with the ALCO Reporting Team in Finance to complete the annual review of brokered deposits. Alternatively, the BSA and ALCO teams should partner to evaluate the possibility of developing an approved list of deposit brokers to ensure the risk is sufficiently mitigated and to possibly minimize the effort required to complete the annual review.

Management Action Plan:
Existing practices will be reviewed, documented at the time of the next risk assessment review beginning in June 2023.

BSA management will revise the procedures to include the rationale for a process and to ensure data is obtained from a reliable source to ensure the information received is complete and accurate. BSA will partner with ALCO Reporting Team for an approved list of deposit brokers. The appropriate associate will be contacted to gather the information pertaining to Brokered Deposits, Demand Deposits and CDs.

Issue Owner(s): Lisa Burkhart and Alanna Williams
Issue Due Date: 09/30/2023

AUDIT ISSUE		
2023 BSA A6	New Account Anticipated Activity Reviews	**Rating**: Low

Background: Anticipated account activity information is collected at the time of account opening through the Customer Due Diligence (CDD) process and is one tool the Bank uses to evaluate an account's risk level. This information is collected for cash and wire activity on all accounts. For any accounts that were assigned a high-risk rating and exceeded their anticipated activity levels by 125 percent or more within the first six months, the BSA Department completes a review of the account to determine what level of high risk they actually exhibit based on transactional behaviors. Once the review is completed, conclusions are documented within Patriot Officer and the risk rating and anticipated activity thresholds within the Bank's core system are adjusted, if needed.

Issue: Internal Audit tested 32 accounts where actual activity exceeded anticipated activity by more than 125 percent within the first six months. Testing revealed the following:

- One instance where documentation of review lacks detail to support risk rating and/or anticipated activity decision. Records indicate a review was performed, but there were no additional notes indicating the conclusion made.
- Three instances where anticipated activity was not updated within the core system as stated in the review conclusion.
- Two instances where the risk rating notated in the review was inconsistent with the data included in the system.

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: Process – Manual Process: The anticipated activity review process is highly manual in nature and requires multiple inputs to various systems increasing the likelihood of human error and data inaccuracies.

Recommendation: We recommend expanding the quality control function to include testing over the anticipated activity review process. A quality control review will assist the Bank in identifying repeat errors timely, provide an opportunity for training, and will be a valuable feedback tool for associates completing reviews. Additionally, we recommend management correct the issues identified.

Management Action Plan:
Corrections of issues identified will be remediated by end of March 2023. Will work with the SAS Team to add fields to Risk Rating Change report to include fields associated with new account reviews.

Issue Owner(s): Teresa Clanton
Issue Due Date: 06/30/2023

AUDIT ISSUE		
2023 BSA A7	Accuracy / Completion of Office Information on Currency Transaction Reports (CTRs)	**Rating**: Low

Background: The Bank is required to report cash transactions over $10,000 completed in a single day by a single individual by submitting a CTR to FinCEN. A CTR includes 57 data fields that are divided into items labeled by FinCEN as critical and non-critical. All critical items must be completed before submission. Non-critical items should be provided if the information is available to the Bank.

The RSSD ID is a critical CTR field. The Federal Reserve assigns a unique identifier to all financial institutions (and branches) called an RSSD ID at the time of branch opening. For all CTRs filed, the Bank includes "RSSD" as the *Financial Institution ID Type* and records the applicable branch assigned RSSD ID. If an RSSD ID number has not been assigned to the branch at the time of the CTR being filed, these fields should be left blank.

For ease of filing, Patriot Officer has the ability to save RSSD ID numbers and addresses for the Bank's branches. Once these fields are updated in Patriot Officer, the associate completing the CTR has the ability to select the appropriate branch location and all related address fields will be completed automatically.

Issue: During our review of thirty-two CTRs we noted the following:

- Two instances where filings included no information reported for *Item 40 - Financial Institution ID Type or ID Number* under *Part III – Transaction Location, although the BSA team had the information*.
- Two instances where filings had inconsistent or missing information noted regarding *Item 40 – Financial Institution ID Number* and *Items 33* through *36 - Address* entered under *Part III - Transaction Location*.

Impact Analysis: Risk of potential violations with BSA and OFAC regulations are not adequately identified and assessed, resulting in an ineffective BSA compliance program, non-compliance, and exposure to regulatory penalties and reputational damage.

Root Cause: People – Understanding & Accountability: There is lack of clarity related to the process of notification of branch location changes (closures, openings, acquisitions, and relocations), requesting/obtaining RSSD IDs for all locations, and making changes to branch location information and RSSD ID numbers within Patriot Officer, within the BSA team.

Recommendation: We recommend management develop a process and assign ownership to ensure an annual review of data accuracy. This process should be documented to ensure consistency and responsibility standards are maintained. Additionally, BSA should partner with Legal to ensure the branch opening checklist is expanded to include notification to BSA so appropriate system updates can be completed timely.

Management Action Plan:

An email was sent to Christy Puckett, Patriot Officer Business Analyst, to complete a review of all office/branch information in Patriot Officer. Any missing RSSIDs and incorrect information has been corrected as of 03/08/23.

BSA Management will contact our Legal Department to ensure the branch opening checklist is expanded to include notification to BSA in order that Patriot Officer is updated with correct information.

Issue Owner(s): Lisa Burkhart
Issue Due Date: 06/30/2023

AUDIT ISSUE		
2023 BSA A8	Annual BSA Training Completion	**Rating**: Low

Background: Banks must provide BSA/AML training for appropriate personnel including both associates and Directors. Training should cover BSA regulatory requirements, supervisory guidance, and the bank's internal BSA/AML policies, procedures, and processes. All associates complete training online through the Bank's Cornerstone OnDemand system while training is provided in person to the Board of Directors. Training completion is monitored by the Learning & Development department of the bank. Associates and leaders receive automated email reminders and notices when training is coming due and has gone past due.

Issue: The following issues were noted when reviewing procedures and performing testing:

- One instance where BSA training was not provided to a Director. The Director was not present at the July 19, 2022, board meeting when training was provided, and training was not provided thereafter.

Impact Analysis: Directors are unaware of key regulatory requirements and potential indicators of money laundering / terrorist financing, resulting in ineffective monitoring and reporting.

Root Cause: Root Cause: Process – Policy & Procedure: The current process for Board BSA training does not include a component to ensure all directors complete required training.

Recommendation: Annual training requirements for Directors should be included on the Director Education tracking report maintained by the Financial Reporting Team and shared with the Board periodically.

Management Action Plan:
BSA Officer will partner with the Financial Reporting team to include annual BSA Training requirements on the Director Education tracking report.

Issue Owner(s): Alanna Williams
Issue Due Date: 09/30/2023

Appendix II: Detailed Controls Tested & Results

Control #	Control Name	Test Steps	Results
CMP 40-01	**Control Name: BSA/AML Enterprise Wide Program Approval** At least annually, or more frequently if needed, the BSA Officer, with support of select BSA Analysts, reviews and updates as needed the Enterprise-Wide BSA/AML Program and Procedures Manual. The updates are approved by the Chief Risk Officer who then presents to the Risk Committee of the Board of Directors (Risk Committee) for approval.	• Verified the organization has overall BSA/AML Compliance Program	Effective
CMP 40-02	**Control Name: BSA/AML Annual Risk Assessment** The Risk Committee approves the risk assessment once approval is granted by the Chief Risk Officer.	• Obtained the BSA/AML and OFAC Risks Assessments • Assessed the BSA/AML and Sanctions Controls • Verified Risk Assessment prepared by BSA Officer Annually • Assessed Risk Assessment methodology • Inquired to ensure Risk Assessment Methodology is reviewed and approved by Senior Management	Exception Noted
CMP 40-03	**Control Name: BSA Officer Appointment-Reconfirmation** Annually, the Board of Directors appoints (or reaffirms) the BSA Officer.	• Confirmed the institution has designated or assigned a BSA Officer.	Effective
CMP 40-04	**Control Name: Monthly BSA Program Metrics** Monthly, BSA Compliance presents BSA Program metrics to the BSA Oversight Committee.	• Verified the BSA oversight committee receives periodic AML Program updates • Obtained and inspected reports used to generate the monthly program updates to assess metrics are accurate reflection of data	Effective
CMP 40-05	**Control Name: Quarterly BSA Program Metrics** Quarterly, the BSA Officer presents the BSA program metrics to the Risk Committee of the Board of Directors.	• Verified the Risk Committee receives periodic AML program updates • Obtained and inspected reports used to generate the monthly program updates to assess metrics are accurate reflection of data	Effective
CMP 40-06	**Control Name: BSA/AML Enterprise Wide Training** Annually, all associates and the Board of Directors are required to participate in Bank Secrecy Act/Anti-Money Laundering training.	• Inspected the HR employee listing to verify that all employees listed are included in employee training tracker	Exception Noted

Control #	Control Name	Test Steps	Results
		• Obtained the employee training tracker, reports management reports, and new hire roster and assessed training completion within 90 days • Obtained and inspected evidence the Board of Directors received and completed annual BSA/AML and OFAC training	
CMP 40-07	**Control Name: BSA/AML Targeted Training** Annually, role-based associates are required to participate in Targeted LOB training.	• Obtained Lines of Business AML training, reports, and attendance tracker and tested co-development with BSA officer and tailoring to job role • Obtained reports and training attendance to verify completion and reporting of non-attendance is escalated to appropriate management	Exception Noted
CMP 40-08	**Control Name: BSA Recordkeeping Requirements** The bank maintains all BSA/AML and OFAC related documentation for at least the minimum length of time (5 years) as required by BSA and OFAC regulations and documents the requirement within its own BSA/AML/OFAC program.	• Verified BSA policies and procedures indicate document retention requirement of 5 years • Obtained selected records/documents and inspected to verify they were retained in line with regulatory requirements	Effective
CMP 40-10	**Control Name: 314(b) Information Sharing** All Outgoing and incoming 314(b) information requests are logged by the BSA Officer or designee for tracking of completion.	• Confirm the bank has a formal process and policy and procedure to designate the Point of contact for 314(b) information sharing, safeguarding confidentiality, proper notice is filed, and the investigations for suspicious activity of matching subjects	Effective
CMP 40-20	**Control Name: CTR Completeness** BSA uses multiple reports to manually aggregate transactions for target clients and verify the completeness of CTRs.	• Verify the bank has a process in place for reporting Currency Transaction Report (CTR). • Verify process and controls in place to group known relationships for CTR reporting purposes • Verify processes are in place to identify clients attempting to structure transactions to avoid CTR filing thresholds	Effective
CMP 40-21	**Control Name: Patriot Officer CTR Alerts** BSA verifies the accuracy of draft CTRs via validating and working Patriot Officer alerts.	• Verify the bank has a process in place for reporting Currency Transaction Report (CTR). • Verify process and controls in place to group known relationships for CTR reporting purposes	Effective

Control #	Control Name	Test Steps	Results
		• Verify processes are in place to identify clients attempting to structure transactions to avoid CTR filing thresholds	
CMP 40-22	**Control Name: CTR Batch File** BSA verify completeness and accuracy of final CTR batch file by comparing information from Teller and Patriot Officer.	• Verify the bank has a process in place for reporting Currency Transaction Report (CTR). • Verify process and controls in place to group known relationships for CTR reporting purposes • Verify processes are in place to identify clients attempting to structure transactions to avoid CTR filing thresholds	Effective
CMP 40-23	**Control Name: CTR Exemptions Monitoring** For clients identified to have potential exemption, a BSA Analyst in the CTR Group performs an assessment to confirm exemption eligibility based on regulatory requirements.	• Verified the institution has established processes and controls that allow the institution to file a "Designation of Exempt Person with the Department of Treasury for Phases I and Phase II Exemptions • Verified monitoring process is in place to review exempt accounts annually • Reviewed BSA policy/procedures to ensure CTR exemption are adequately documented	Effective
CMP 40-24	**Control Name: CTR Exemptions Review** Annually, a BSA Analyst in the CTR Group completes the review of the eligibility of an exempt person that is a listed public company, a listed public company subsidiary, a non-listed business, or a payroll customer to determine whether such person remains eligible for an exemption. All confirmed exemptions are reported to the BSA Oversight Committee.	• Assessed exempt CTR clients to ensure the customer meets the criteria, annual review completed, and any changes are executed on the core system • Obtained BSA oversight committee reporting material to confirm results of CTR exemption annual review were presented.	Exception Noted
CMP 40-25	**Control Name: Monetary Instruments** Annually, a BSA Analyst in the CTR Group completes the review of the eligibility of an exempt person that is a listed public company, a listed public company subsidiary, a non-listed business, or a payroll customer to determine whether such person remains eligible for an exemption. All confirmed exemptions are reported to the BSA Oversight Committee.	• Inquired the types of monetary instruments and their purchase restrictions • Reviewed policies and procedures for inclusion requirements to purchase monetary instruments. • Verified period monitoring of monetary instruments sold for potential activity • Verified all required information is recorded and accurate in the log of purchases and sales of monetary instruments	Effective

Control #	Control Name	Test Steps	Results
		• Inspected evidence to confirm instruments are only sold to customers • BSA Officer approved sale of monetary instrument if MI sold to non-client	
CMP 40-30	**Control Name: Transaction Monitoring – Alerts Review** BSA Alert Analysts investigate Patriot Officer Alerts for potentially suspicious activity.	• Inquired with management regarding the bank's process for automated transaction monitoring alert management • Obtained and inspected BSA policy/procedures to assess whether transaction monitoring alert management process is adequate • Confirmed alerts are investigated, and rationale provided is adequate • Verified alert was decisioned timely	Exception Noted
CMP 40-31	**Control Name: Transaction Monitoring – PO Rules Review** Patriot Officer rules set is evaluated by the BSA/AML Manager to identify and make updates to underperforming rules and thresholds.	• Obtained documentation for new or updated transaction monitoring rules and alert configurations	Effective
CMP 40-32 & CMP 40-33	**Control Name: Transaction Monitoring – Escalated Alert Review, Manual SAR Referrals, Final SAR Decisioning** BSA SAR Analysts investigate escalated Patriot Officer alerts and manual SAR referrals for suspicious or unusual activity and file a SAR as needed.	• Confirmed the bank has policies and procedures in place for identifying suspicious activity including lines of communication, destination of individuals, procedures for reviewing and evaluating the transaction, the SAR decision process, investigation files confidentially maintained, rationale behind decisions not to file SAR, evidence of management review and approval, escalation issues identified, completion, filing, and retaining of SARs, and appropriate research measures • Confirmed formalized process for completing and filing SARs • Validated the adequacy of policies and procedures regarding suspicious activity reporting • Confirmed with management that SAR filings are stored in secure location	Effective

Control #	Control Name	Test Steps	Results
CMP 40-34	**Control Name: SARs Filed – 90 day Follow up Review** When a SAR decision cannot be reached by the SAR Analyst, the AML Manager or BSA Officer has the final decision-making authority.	• Obtained and inspected policy and procedures to confirm that process information is adequately documented • Confirmed formalized process for completing SARS • Confirmed account closing procedures and approvals are required because of continuous suspicious activity • Obtained a sample of 90-day reviews and validated appropriate information included, verified timeliness of reviews, and confirmed client relationship was exited in a timely manner if second SAR was filed	Effective
CMP 40-35	**Control Name: BSA Compliance QC – Alerts Review** Monthly the Quality Control QC Manager and Team, perform a sampling review of alerts "justified no" by the Alert Analyst team to verify quality of the investigation and if the decision to not escalate the alert for further review and/or SAR filing was properly supported.	• Inspected QC procedures and guidelines for established process to review alerts • Assessed QC results documentation, retention, and communication • Determined results are analyzed for trends and potential training needs • Validated alerts were reviewed by QC lead • Validated alerts were selected by QC lead based on established guidelines	Effective
CMP 40-36	**Control Name: BSA Compliance QC – SARs Filed Review** Quarterly, the Quality Control QC Manager and Team use the SAR Report Log and a report in Patriot Officer to identify SARs filed, SAR 90-Day Reviews, and escalated alerts "justified no" worked by SAR Analyst team in prior quarter.	• Reviewed manual to ensure process was documented • Validated the selected SARs (based on guidelines) were reviewed • Verified the QC review and conclusion were documented and completed timely • Confirmed the quarterly report was communicated appropriately • Assessed whether remediation plan was prepared and communicated appropriately if issues were identified during QC review	Effective
CMP 40-37	**Control Name: Risk Rating Reviews**	• Met with management to identify required Customer Due Diligence (CDD) documentation required for account opening	Exception Noted

Control #	Control Name	Test Steps	Results
	Monthly, BSA Risk group reviews new accounts opened 6 months prior, for accurate assessment of anticipated activity and assignment of risk rating.	• Reviewed the Bank's CDD policies and procedures • Verified established procedures for resolving issues • Ensured procedures in place for periodic reviews of accounts and understanding the purpose of relationship • Assessed whether the bank had adequate risk-based procedures for updating customer information, including beneficial ownership • Validated presence of CDD information in Core system	
CMP 40-38	**Control Name: High Risk Account EDD Review Completeness** Monthly, BSA Risk group reviews SAS-High Risk Account Reports to verify EDD/Reviews are complete.	• Confirmed methodology used to risk rate customers and the periodic reassessment pf risk ratings • Verified BSA program provides guidance to identify "higher risk" clients • Determined if EDD policies and procedures are in place to gain sufficient knowledge of potential clients, the bank has procedures in place to change risk ratings, and there are periodic reviews of anticipated activity • Verified the BSA Officer has mechanism in place to track customers identified as high risk and that the bank performs additional due diligence on high-risk clients • Verified EDD and CDD information obtained at account opening and reviewed in a timely manner • Reviewed transaction history for appropriateness compared to risk profile	Exception Noted

CMP 40-39	**Control Name: 314(a) Positive Match Reporting**
	Bi-weekly, BSA Risk Analysts report positive matches to FinCEN and SAIFs to BSA AML Manager.
		• Confirmed the bank has a formalized process, policy, and procedure for
		  ○ Point of contact for 314(a) requests
		  ○ Sending and responding to requests
		  ○ Safeguarding and information confidentiality
		  ○ Investigating matches
		  ○ Searching account matches
		  ○ Maintaining documentation
			Effective

Control #	Control Name	Test Steps	Results

		• Validated accuracy of policies and procedures regarding 314(a) information requests
		• Verified upload of 314(a) requests were
		  ○ Uploaded timely
		  ○ Researched timely
		  ○ Were properly documented
		  ○ Escalated to SAR group as needed
		  ○ Sufficiently documented and evidenced
		  ○ Were reported to FinCEN within 14 days if a positive match	

CMP 40-40	**Control Name: Weekly OFAC Batch Review** The BSA Risk Manager or analyst reviews all OFAC batches from the prior week, to ensure accuracy and report to OFAC timely.	• Confirmed the bank has a formal process for complying with OFAC laws and regulations • Confirmed alerts were closed and rationale was adequate • Verified the alerts were investigated and closed in a timely manner • Confirmed true matches were reported to FinCEN within 10 days.	Effective
CMP 40-41	**Control Name: OFAC SDN List Management** Quarterly, the BSA Risk Manager or designee will compare Patriot Officer SDN list of changes to the US Department of Treasury list of changes.	• Reviewed OFAC policies and procedures regarding OFAC lists, internal watchlists, and vendor provided lists • Determined policies and procedures adequate regarding change management • Confirmed the U.S. Department of Treasury OFAC Sanctions list corresponded to update on Patriot Officer list maintenance file • Confirmed update was performed timely	Effective
CMP 40-42	**Control Name: WITS Deny List** The BSA Risk Manger or designee verifies the WITS Deny List was updated correctly.	• Confirmed the bank has adequate processes to comply with Section 311 of the USA Patriot Act • Obtained screenshots of the bank's monitoring parameters • Assessed Compliance monitoring policies and procedures are comprehensive and adequate	Effective
CMP 40-43	**Control Name: Quarterly High Risk RDCC Reviews by BSA**	• Confirmed the following	Exception Noted

Control #	Control Name	Test Steps	Results
	On a quarterly basis, BSA reviews a sample of high-risk remote deposit clients and reports observations that fall outside of the RDC client review standards, to the Treasury Management Performance Director, the Treasury Management Advisor and Financial Advisor.	○ RDC clients have established transaction limits ○ Expected account activity is obtained from RDC clients ○ Actual account activity is periodically compared to expected activity to ensure reasonableness ○ Significant changes in transaction activity results in additional monitoring • Confirmed BSA manager reviewed a sample of high risk RDC clients quarterly	
DO 10-1 and LO 09-05 Series	**Control Name: Account Opening Requirements – NCIP** New accounts entered into the deposits accounting system are independently reviewed by Quality Control for critical attributes For each booked loan, the Commercial Credit Services QC team verifies the completeness of loan documentation. Retail Lending Quality Control team (QC) completes a QC checklist to verify the accuracy and completeness of each loan package. Post closing team reviews each loan package for accuracy and ensures all documentation is properly executed before it is booked or shipped. SBA Closing Advisors verifies setup accuracy of all SBA loans booked in PCFS Loan Manager, by SBA Operations Analyst bookers, by comparing the data fields per Loan Manager to loan documents. NC Loan Operations verifies setup accuracy of 1) participation fields only of all Participations Bought, booked in JH Silverlake by Commercial Credit Services group, and 2) all Participations Sold loans booked in JH Silverlake by bookers within the NC Loan Operations group, by comparing the data fields per Silverlake to the loan documents using the New Verification Checklist, and	• Inspected CIP and related procedures to determine alignment with regulatory requirements • Determined whether policy and procedures ○ require client identification verified timely ○ allow accounts to be opened without all required customer information and verification • Verified the firm notifies clients that it will seek identification requirements (31 CFR 1020.220 (a)(5)ii) • Validated required CIP information on file • Determined if documentary or nondocumentary method of identification used and on file • Validated accuracy of CIP information on file • Validated OFAC screen performed on new clients • Verified Beneficial Ownership form on file as applicable • Inspected KYC collected and retained	Effective

Control #	Control Name	Test Steps	Results
	3) all bought tranches booked under an existing bought line of credit booked by the TN Loan Operations group, by comparing the data fields per Silverlake to the loan documents using the New Verification Checklist		
CMP 40-XX BLK	**Control Name: Annual Blocked Transaction Report** Annually, the Report on Blocked Property is reviewed by the BSA Officer or designee and filed with OFAC by September 30.	• Confirmed the bank established and maintains adequate policies and procedures for handling transactions blocked under OFAC • Obtained and reviewed the bank's blocked transaction list to assess whether documentation is adequate and is retained at least 5 years • Confirmed funds were held in appropriately titled interest-bearing account • Confirmed withdrawn funds were approved by FinCEN • Verified fees charged appeared reasonable • Confirmed FinCEN was notified of blocked transactions within 10 days • Confirmed items included on annual report filed with FinCEN no later than 9/30/2022	Effective
BD	**Control Name: Brokered Deposits** Annually, the BSA CTR Manager conducts a review of all brokered deposits to confirm compliance with regulatory guidelines.	• Validated the following ○ BSA Program includes policies, process, and procedures related to brokered deposit relationships ○ Management effectively identifies and monitors brokered deposits ○ The bank's system for monitoring and reporting suspicious activity is adequate given the risk, size, and complexity of the organization	Exception Noted
CMP 40-X-OG	**Control Name: Regulatory Change Management** Appropriate change management and documentation protocols are in place to ensure corrective action and compliance program changes are tracked and escalated.	• Verified process is in place to track and store AML issues and compliance program changes • Verified issues requiring corrective action and compliance program changes were tracked and escalated, when necessary	Effective

Control #	Control Name	Test Steps	Results
		• Verified appropriate process owner, reasonable action plan, and target dates were documented for selected regulatory change items • Obtained and reviewed evidence to confirm action plan was effectively implemented	
SAO	**Control Name: Subsidiary and Affiliate Oversight** Annually, the BSA Officer conducts firm-wide BSA/AML Risk Assessment that covers the risk and risk mitigation measures for each of the Bank's subsidiaries and considers the bank's affiliates (BHG). Oversight activities related to each of the bank's affiliates and subsidiaries is dependent upon the activities of the entity and related risk to the enterprise.	• Confirmed the following ○ BSA/AML Enterprise Risk Assessment includes all Subsidiaries and affiliates ○ Oversight and risk management activities are reasonable ○ AML Program attestation are received by BSA Officer	Exception Noted
TPPP	**Control Name: - Third Party Payment Processors** Annually, an Enhanced Due Diligence form and a Credit Review is performed on Third Party Payment Processors.	• Evaluated adequacy of policies, procedures, and processes related to third party payment providers • Determined the bank effectively identifies and monitors processor relationships including suspicious activity monitoring and reporting • Reviewed account opening document and ongoing due diligence information • Reviewed transactions/statements to compare expected transaction volume to actual transaction volume • Assess controls concerning identification of high rates of returns	Effective
MO	**Control Name: Model Oversight** Biannually, the Bank performs model validation testing on all applicable BSA/AML and OFAC models. Results are reviewed by the BSA Officer or designee and reported to the Board of Directors.	• Confirmed the following ○ Model owner executes model activities that ensure completeness, accuracy, and appropriateness of model inputs and outputs ○ Model validation findings are evaluated and tracked for remediation ○ There are no significant findings outstanding ○ Model changes are approved by appropriate parties, reported to	Effective

Control #	Control Name	Test Steps	Results
		management, and documented on the model change control log	

Appendix III- Definitions

Issue Ratings:

Critical: An issue that should be given the highest priority and addressed immediately. These represent both a systemic and immediate threat to the organization as they relate to the existence, strategy, and business model of Pinnacle Financial.

High: An issue or combination of issues that have or could have a serious impact to Pinnacle Financial, its customers or third parties. These represent a severe exposure that is impacting the achievement of management objectives. They can result in, but are not limited to, substantial monetary loss, serious reputation damage, significant adverse regulatory impact, and serious violations of company policy.

Medium: An issue or combination of issues that have a substantial impact to Pinnacle Financial, its customers or third parties. These represent a considerable exposure that is likely to impact the achievement of management objectives.

Low: An issue or combination of issues that have a low impact to the Company, its customers or third parties. These represent a noticeable but low exposure that could hinder the achievement of management objectives.

Audit Entity Report Ratings:

Satisfactory: The overall strength of the control environment provides reasonable assurance that risks are appropriately managed for the scope of the audit. A few control issues of lower significance may exist. Risk has been managed at a generally acceptable level. Non-compliance with policies, standards, and procedures, including regulatory requirements, is minimal.

Satisfactory with Recommendations: The overall strength of the control environment and management of risk has some deficiencies, but certain activities and risks are well controlled. Risk has been managed at a generally acceptable level although management should enhance control activities to avoid adverse operational impact, reputation damage, and/or financial loss. Some areas of minimal non-compliance with policies, standards, and procedures, including regulatory requirements were noted.

Needs Improvement: The overall strength of the control environment and management of risk has some significant deficiencies, or several deficiencies that collectively aggregate to a significant deficiency, but certain activities and risks are well controlled. Risk exposure is meaningful in select areas and requires management's prompt attention and corrective action to limit or avoid adverse operational impact, reputation damage, and/or financial loss. Some areas of significant non-compliance with policies, standards, and procedures, including regulatory requirements, were noted. Repeat issues may be evident.

Unsatisfactory: The overall strength of the control environment is poor and has multiple significant weaknesses within the scope of the audit, resulting in an unacceptable level of risk. Exposure is extensive and requires management's immediate attention and corrective action to limit or

avoid adverse operational impact, reputation damage, and/or financial loss. Non-compliance with policies, standards, and procedures, including regulatory requirements, is substantial. Repeat issues, if any, are of a significant nature.

Root Cause:

Category	Contributing Factor	Definition
Governance	**Strategy**	Objectives, strategy, vision, assumptions or required outcomes are unclear or failure to respond quickly to changes and emerging issues.
	Structure	Board, committee, or business organization is inadequate or inappropriate
	Culture	Culture, including staff engagement, promotes risk-taking beyond that of the organization's agreed risk appetite
People	**Competency**	Inadequate ownership, skills, competencies, training, experience, or knowledge
	Resources	Insufficient staff (level or number), budget resources, tools, or time; lack of planning/prioritization; conflicting or competing priorities
	Understanding & Accountability	Staff duties, responsibilities, authorization, delegations, or segregation of duties are not understood by staff and/or leadership oversight and accountability related to such is lacking.
Process	**Policy & Procedure**	Ineffective policy and establishment of controls and procedures, setting, oversight, monitoring, follow-up, or enforcement
	Manual Process	Process is highly manual in nature, requires high degree of judgment to determine appropriate inputs and/or involves multiple hand-offs between owners and lines of business that may result in data quality concerns
	Third Parties & Vendors	Third party delivery/control failure or dispute, inadequate oversight, and monitoring
	Change Management	Implementation of a new/changed product, service, process, or system is inadequate
Technology	**Design**	Design in ineffective, inefficient, or overly complex
	Integration or Obsolescence	System is not integrated across the enterprise, which could lead to functionality or data quality concerns, or legacy/obsolescent system
	Maintenance	Inadequate change management or maintenance
	Security	Security, access control, or data protection is inadequate