Federal Deposit Insurance Corporation
New York Regional Office
350 Fifth Avenue, Suite 1200, New York, New York 10118

NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES
One State Street, New York, New York 10004

Apple Bank for Savings Supervisory Letter #03-2020

November 5, 2020

Board of Directors
Apple Bank for Savings
122 East 42nd Street
New York, NY 10168

Subject: Information Technology (IT) Target Supervisory Letter

Dear Board Members:

This letter summarizes the findings of the April 27, 2020 IT Target Review (Target Review) of Apple Bank for Savings (Bank). The review was a joint effort by the Federal Deposit Insurance Corporation (FDIC) and the New York State Department of Financial Services (NYSDFS). This Letter and its contents, including attachments, are confidential and intended only for the Bank's internal use. The disclosure of such confidential supervisory information is governed by Part 309 of the FDIC Rules and Regulations and Section 36.10 of the New York Banking Law. This letter should be afforded the same level of attention as a Report of Examination.

SCOPE

This Target Review evaluated the Support & Delivery component of the Uniform Rating Systems for Information Technology (URSIT). Examiners also assessed the Information Security (IS) and Cybersecurity programs, as well as conformance with Appendix B to Part 364 of the FDIC Rules and Regulations - Interagency Guidelines Establishing Information Security Standards. NYSDFS examiners performed a concurrent review of compliance with the NYSDFS Cybersecurity Requirements for Financial Services- 23 NYCRR 500 (Part 500). Examiners also reviewed the remediation status of previous Matters Requiring Board Attention (MRBAs) and Supervisory Recommendations (SRs). The 2021 IT Target Review will include a full assessment of the Audit, Management, and Development & Acquisition areas.

UNIFORM RATING SYSTEM FOR IT (URSIT) - 2

	Current Exam*	Prior Exam	Prior Exam
Target Exam Date	4/27/2020/ J	1/28/2019/ J	2/26/2018/J
Composite Ratings	2	2	3
Component Ratings			
Audit	2	2	2
Management	2	2	3
Development & Acquisition	2	2	2
Support & Delivery	3	3	3

* The rating assigned to the Support & Delivery component is based on the results of this Target Review. The ratings assigned to the Audit, Management, and Development & Acquisition areas are carried forward from the 2019 IT review. Management is appropriately addressing prior supervisory recommendations. Examiners and specialists utilize continuous monitoring practices to assess emerging risks, analyze changes in business strategy, and monitor corrective action. Any significant changes will be addressed with bank management, as necessary.

Uniform Rating System for Information Technology Ratings Definition - 2

Financial institutions and service providers rated composite "2" exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates, but responds less quickly, to changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.

SUMMARY

IT performance and Board and senior management oversight remain satisfactory. However, supervisory concerns remain within the Support and Delivery function, including: the IT enterprise-wide risk management program; identification and documentation of key controls; hardware and software inventory; end-of-life (EOL) management; server and workstation hardening standards; monitoring of security events; and privileged user reviews. The Information Security Program (ISP) framework provides reasonable assurance that IT and Information Security (IS) risks are identified. However, the Bank is not in conformance with *Part 364, Appendix B, of the FDIC Rules and Regulations.* Cybersecurity risk is adequately identified. Management, however, self-reported nonconformance with the requirements of NYSDFS Part 500 to the Board Risk Management Committee and to NYSDFS in the Part 500 Cybersecurity Certification dated May 22, 2020.

Gramm-Leach-Bliley Act (GLBA) Conformance

Despite management's continued efforts towards developing an appropriate risk assessment framework and program, the Bank remains in nonconformance with the Interagency Guidelines Establishing Security Standards pursuant to Section 501 (b) of the GLBA of 1999, as set forth in Part 364, Appendix B, of the FDIC Rules and Regulations. IT-related risk assessments do not adequately inform or guide risk mitigation and management. Since management is working on new risk assessments, proper control testing has not yet been conducted. Appendix B to Part 364 of the FDIC Rules and Regulations mandates that the Bank regularly test independently the key controls, systems, and procedures of the information security program. Refer to Appendix A - Violations of Laws and Regulations for additional information.

Management Response: Chief Risk Officer (CRO) Steven Eckert is responsible for the establishment of an appropriate GLBA Risk Assessment Framework, and the identification and testing of the key controls. Negotiations have commenced with ITA Partners to assist management with establishing an effective GLBA Risk Assessment, and establishing and testing the key controls. Management plans to have the GLBA Risk Assessment and the identification and testing of the key controls completed by September 30, 2020. The target date to present the GLBA Risk Assessment to the Management Risk Committee and approval by the Board Risk Committee is October 28, 2020.

Cybersecurity Preparedness

The Cybersecurity Program is not in full conformance with the requirements of NYSDFS Part 500. In January 2020, the Bank hired a new Chief Information Security Officer (CISO), Maksim Tumarinson, who needed to determine the current state of the Bank's cybersecurity program prior to performing the formal certification. When performing the Cybersecurity Certification process for calendar year 2019, CISO Tumarinson identified gaps that were not previously identified in 2018. The gaps and corrective action plans were presented to the Board Risk Committee in March 2020, and sent to the NYSDFS in the Bank's Part 500 Cybersecurity Certification dated May 22, 2020. This certification identified where the Bank failed to fully comply with some of the requirements of the Regulation in sections: 500.02-"Cybersecurity Program"; 500.06–"Audit Trail"; 500.07–"Access Privileges"; 500.09–"Risk Assessment"; 500.12–"Multi Factor Authentication"; and 500.13–"Limitations on Data Retention". Nonconformance with these sections stems primarily from an inaccurate application inventory. This is being remediated by CISO Tumarinson. Furthermore, the noncompliance with 500.14–"Training and Monitoring"; 500.15–"Encryption of Non Public Information"; and 500.16 –"Incident Response Plan", was also self-reported and is in-process of remediation. The Bank has plans in place delineating steps to become fully compliant with Part 500.

Management Response: CISO Tumarinson indicated that the partial nonconformance in sections 500.02; 500.06 – 500.07; 500.09; 500.12– 500.13 should be fully remediated by September 30, 2020, and nonconformance with 500.14 - 500.16 will be remediated, and be brought into full compliance by December 31, 2020.

STATUS OF PRIOR FINDINGS

One of the two MRBAs issued at prior Target Reviews was adequately addressed and closed. Additionally,

four of the nine SRs outstanding from prior Target Reviews have been addressed and closed. Moreover, examiners cited five new SRs related to network monitoring, user access rights administration, database management, network access control, and change control. Refer to the Supervisory Recommendations section of this letter and *Appendix B – Summary of Regulatory Issues* for additional information.

IT ORGANIZATIONAL CHANGES

New senior management was hired in an effort to address prior audit and regulatory examination findings and strengthen leadership of the IT and IS departments. Chief Technology Officer (CTO) Debi Gupta was elevated to his new position on March 4, 2020 and CISO Tumarinson was hired on January 6, 2020. AVP David Camposano was hired on April 20, 2020 to take over Business Continuity Planning/ Disaster Recovery and FVP Holly Amorosana was recently hired as the Chief Privacy Officer.

Since ascending to the CTO position, Mr. Gupta has worked to create relationships with both the second line of defense (Information Security), and the third line of defense (Internal Audit). These relationships led to an agreement to provide information to Internal Audit (IA) within 5 days or less per request to be able to clear audit findings and address additional information requests in a timely manner. This increased communication has led to timely closure and validation of IA findings as well as a comprehensive and aligned formal tracking methodology between IA and IT. According to CTO Gupta the primary focus is on addressing prior issues. However, the completion of future projects such as data warehousing and IT architecture will be prioritized based on risk level.

CISO Tumarinson reports to CRO Ekert. Mr. Tumarinson has the necessary experience to lead the Information Security Department commensurate with the Bank's size and complexity. CISO Tumarinson has worked on building relationships with stakeholders, most importantly IT, as well as retail banking and other areas. He established the InfoSec Cyber Risk Committee, comprised of all business units, to ensure proper time is allotted to address all outstanding information security issues. The Bank's IT Workplan states that the initial focus of CISO Tumarinson will be to address the outstanding regulatory and internal audit findings.

PANDEMIC RESPONSE

Senior management and members of the Bank's Executive Management Steering Committee (EMSC) began to monitor the potential impact of the Coronavirus on Apple Bank's operations in mid to late February 2020. This included participating in industry calls with the American Bankers Association, the Mid-size Banking Coalition of America, and external consultants. On March 3, 2020 the Bank began to send communications to its staff about the Coronavirus and the steps that staff should take to help reduce the spread of the virus. Beginning on March 5, 2020, the Bank's EMSC began meeting on a regular basis. The Bank developed and implemented a remote access strategy by the end of March 2020 that allowed essential employees to perform all critical functions remotely. By the beginning of April 2020, the Bank moved approximately 450 back office and headquarters operations staff to a remote-work environment including SWIFT and the Wire Room. The Bank has taken steps to ensure its call center remains operational and as many branches as possible remain open throughout the

pandemic. The Bank is adjusting hours of operation to minimize social interaction and to ensure branches are properly cleaned and sanitized. As part of the Bank's Coronavirus response, the Bank has been in communication with its high-risk vendors to ensure the vendors have tested plans in place and have the ability to continue to provide required services. The Bank's functions have continued to operate with limited disruptions, including the Bank's main data center which runs the Bank's core applications.

SUPPORT & DELIVERY – 3

IT support and delivery continues to be less than satisfactory. Control deficiencies exist throughout the environment that, if left uncorrected, could cause performance disruption or service degradation. Prior examination findings regarding IT Enterprise-Wide Risk Management Program, identification and documentation of key controls, inventory and EOL management, hardening standards, security event monitoring and privileged user reviews remain outstanding. Furthermore, examiners identified new deficiencies in the areas of network monitoring, user access rights administration, database management, network access control, and change control. Moreover, the Business Continuity Management (BCM) Program was rated Unsatisfactory in the February 26, 2020 Internal Audit Report. The new BCM Program Manager AVP David Camposano has resigned since the conclusion of this Target Review. Controls over the electronic banking activities are satisfactory. Refer to the Supervisory Recommendations section for additional information.

SUPERVISORY RECOMMENDATIONS

Previous Target Review Matters Requiring Board Attention

MRBA #04– 2016 IT Enterprise-Wide Risk Management Program (IT-ERMP)

Corrective Action: Management should enhance the IT risk assessment program and fully develop the IT risk management framework needed to support the IT –ERMP.

Supporting Comment: Former CTO Aditya Kishore completed risk assessments since the 2019 Target Review contracting Wolf and Company. However, the resulting work product was determined to be insufficient by Senior Management. The methodology used applied a standard set of risks and controls to all the individual IT assets resulting in a 1000 page IT Risk Control Self-Assessment (RCSA) that did not provide identification of control gaps or a prioritized list of action items. Moreover, the proprietary methodology used to measure inherent and residual risks and control effectiveness of each of the IT assets provided no reference for the Bank to evaluate this analysis. Risk assessments should use qualitative measures and provide an easy to understand analysis of Bank-specific IT risks. To ensure the timely identification and mitigation of risk exposures, management should update the risk assessments regularly to address changes in technologies, products, and services. An all-inclusive risk assessment is necessary to accurately identify and assess risk exposure and prioritize mitigation efforts.

Management Response: CTO Gupta signed an agreement with ITA Partners, a consulting firm that

specializes in Risk and Governance frameworks. ITA Partners will assist the Bank with the IT RCSA process and will work with key stakeholders such as IT and the Risk and Compliance Department. This process is expected to be completed by June 2020. Weekly meetings commenced on March 26, 2020 to discuss the overall IT RCSA process and core functions. The seven IT RCSAs are within the projected timeline with two completed, three underway, and two commencing before June 1, 2020. Bank senior management is reviewing this project on a bi-weekly basis, with the IT-ERMP targeted for approval by the Board Risk Committee in July 2020.

Previous Target Review Supervisory Recommendations

SR #07 – 2016 Identification and Documentation of Key Controls

Corrective Action: Management should identify and document the controls within the Bank's environment. The controls should be used for reporting and testing across the three lines of defense.

Supporting Comment: Currently, IT risk assessments are incomplete and management has not satisfactorily identified and documented key controls. Once the IT-related risk assessments are complete, independent control testing should be performed to validate all key controls are operating as intended. Control testing is a valuable tool for documenting the robustness in controls, identifying and mitigating control gaps, as well as gaining on overall understanding of the risk exposure to existing, expected, or severe events.

Management Response: CTO Gupta indicated that as part of the IT RSCA engagement, ITA partners is conducting sample testing of the key controls. The sample testing is expected to be completed by June 30, 2020 and presented to the Management Risk Committee and Board Risk Committee in July 2020.

SR #01 – 2018 Inventory and End-of-Life (EOL) Management

Corrective Action: Management should strengthen oversight over software and hardware inventory. Management should define a formal process to assess the significance of hardware and software to allow appropriate time to remediate any EOL issues prior to the end-of-support date.

Supporting Comment: Management initiated a process to remediate EOL issues; however, oversight of software and hardware inventory continues to need improvement. The IT Department maintains a software and hardware inventory in the form of several different lists; however, there is no process to ensure all hardware, software, and operating systems are accurately documented. Without a complete enterprise-wide inventory, management cannot effectively identify systems that need additional protection, establish action plans to address EOL issues, or track system changes and available updates. Accurate inventory and appropriate EOL oversight can improve security strategies and reduce the potential attack surface.

Management Response: CTO Gupta indicated that CMDB is an asset management application that will scan the Bank's IT environment to discover, manage, and report on all of the Bank's IT assets. The CMDB discovery tool will ensure that all devices are managed centrally. Formal EOL management

processes will use the data from the CMDB to allow appropriate time to remediate any EOL issues prior to the end-of-support date. The bank has deployed the CMDB system utilizing the ServiceNow platform with automated network scans running nightly to ensure discovery of the entire Bank's IT universe. Although discovery is fully automated, some of the internal processes are still manual. Management is working with the vendor, CDI, to build the roadmap to automate the manual process and this will include licensing and deployment of software asset management systems to address the EOL issues. This project is managed by the Enterprise Project Manager Office and the target date for completion is December 31, 2020.

SR #02–2018 Hardening Standards

Corrective Action: Develop hardening standards for all infrastructure assets and regularly review the infrastructure for compliance with various build standards.

Supporting Comment: Hardening standards for all routers, switches, servers, and Windows workstations were developed and approved by former CTO Kishore. However, CISO Tumarinson has not completed a review of the current standards to ensure the adopted standards are appropriate for the Bank. CISO Tumarinson should review hardening standards for all infrastructure assets, which include windows and network applications, web services, multi-functional printers, databases, etc. CISO Tumarinson should also review and validate that the accepted CIS standards are implemented and align with the Bank's Risk Appetite Statement. The process of developing and maintaining hardening standards strengthens the Bank's systems against information security threats.

Management Response: CISO Tumarinson and IT Department are working together to identity the specific CIS standards that the Bank cannot adhere to and are working through the Risk Acceptance Process. Management has completed the Windows, Cisco, SQL server and VMware CIS certification process. Management is also designing a mitigation strategy for the multi-function printers to establish appropriate hardening standards. Management expects this to be completed by June 30, 2020.

SR #01 – 2019 Security Event Monitoring

Corrective Action: Management should ensure that all security logs are processed through the Security Information Event Management (SIEM) software and anomalous activity is detected in a timely manner.

Supporting Comment: Management previously installed Alienvault SIEM software. However, security logs from each technology source are not yet integrated into the SIEM; most notably logs from MISER. The IT Department should complete the integration of all security logs and develop documented processes for sending security logs to the SIEM when new devices are set up. Finally, CISO Tumarinson and IA should validate that all security logs are captured by the SIEM. To address this issue, former CTO Kishore executed a 7-year contract with FIS to create and manage a SIEM for the bank. In February 2020, after extensive discussions with FIS, senior management determined that the agreement with FIS did not meet its IS requirements. As a result, the agreement was terminated, leaving the Bank with the existing Alienvault solution. A comprehensive SIEM monitoring program allows for greater visibility into possible intrusions

and security violations.

Management Response: CISO Tumarinson has identified several key system logs that were not directed to the SIEM application for event correlation. Weaknesses still exist regarding missing assets and event sources. Based on self-identified limitations with the current Alienvault SIEM, management is upgrading to a cloud based solution. This will allow for expanded host and event logging capacity. Management plans to migrate to the new cloud based solution by October 31, 2020. Additional applications such as workstation logs, Gmail, OKTA, DLP logs will be integrated into the SIEM event monitoring process after the migration is complete.

SR #03 – 2019 Privileged User Reviews

Corrective Action: Management should conduct detailed entitlement reviews on privileged users for all applications quarterly. In addition, the CISO should provide oversight to ensure reviews of all privileged users are performed and the depth of the review is adequate.

Supporting Comment: The ISP requires privileged users to have two User IDs, one for normal business access and one for network administration access, to perform specific system administration work. Using privileged access IDs for normal business purposes increases the risk of privileged user credentials being compromised. Privileged user access reviews should be conducted to determine the appropriate use of the accounts and if any users should be removed for inactivity. Former CISO Frank Grochowski identified 21 applications that are required to be reviewed under the privileged access review on a quarterly basis. He developed the framework and rules of engagement for the review process. IT Security Operations used this framework to complete the privileged user access review for the 21 applications identified. While CISO Tumarinson expanded the review to 46 applications and reduced the number of Active Directory administrators from 16 to five, no monitoring of privileged user account activity has been implemented. Privileged users hold the keys to the bank's most sensitive, confidential, and critical data as well as have the ability to download, alter and delete data. Failure to monitor privileged users can affect the confidentiality, integrity and availability of systems, applications and databases. Management should define critical applications for privileged user monitoring.

Management Response: CISO Tumarinson stated that a list of critical applications will be completed by December 31, 2020. The Privileged Access Management (PAM) solution will be implemented with Log and Event IDs, and Active Directory by March 31, 2021. A plan for other critical applications not in the SIEM will be completed by March 31, 2021.

<u>Current Target Review Supervisory Recommendations</u>

SR #1-2020 - Network Monitoring

Corrective Action: Management should monitor the internal and external network of the Bank.

Supporting Comments: The Bank only monitors the network during business hours. Monitoring the

network 24/7 is critically important because it gives full network visibility and control and screens the network for security threats. Alerts should be generated for any malware present on the systems, abnormal data transfers, or failing systems. Furthermore, 24/7 monitoring will give the Bank valuable security information about network devices (e.g. routers, switches and firewalls) and ensure critical network servers are consistently available.

Management Response: CTO Debi Gupta and CISO Tumarinson stated that they will monitor security events through the SIEM software. Management will contract a Network Operations Center (NOC) vendor by December 31, 2020.

SR #2-2020 - User Access Rights Administration

Corrective Action: Management should implement Role Based Access Control (RBAC).

Supporting Comments: The current paradigm at the Bank has business owners responsible for implementing security for each application they manage. User access right provisioning is based upon the employee's manager's approval, without taking into consideration any other access or permission that the employee might have in other applications or systems. The lack of oversight of user access rights between applications could result in possible toxic combination. Managing application access is essential to information security. With RBAC, security will be managed at a level that will provide visibility across applications and systems within the IT environment.

Management Response: CTO Gupta and CISO Tumarinson agree with the recommendation; however, implementing RBAC is a complicated undertaking requiring substantial human and financial resources. Management will analyze the steps necessary to complete RBAC and will present a business case to executive management by June 30, 2021.

SR #3-2020 - Database Management

Corrective Action: Management should assess and implement field level logging and monitoring of key databases.

Supporting Comments: Management has not established requirements covering the confidentiality, availability, and performance for key databases or key data elements. Databases containing Non-public Personal Information (NPPI) or other confidential information should be assessed to determine whether specific data elements need to be monitored for any unauthorized modifications. The GLBA risk assessment process should address databases with NPPI data and any needed data integrity controls. Management reported that native logging is performed within the SQL server environment; however, specific event monitoring has not been defined. Unauthorized data element changes can result in inaccurate or data integrity issues, which can be identified by field level monitoring.

Management Response: CTO Gupta and CISO Tumarinson stated that both the SIEM and Privileged Access Monitoring (PAM) systems need to be operational in order to implement field level logging and

monitoring of key databases. PAM is targeted to be implemented by March 31, 2021. Management plans to assess and implement field level logging and monitoring of key databases by September 30, 2021.

SR #4-2020 - Network Access Control (NAC)

Corrective Action: Management should implement Network Access Control to protect the network from unauthorized devices.

Supporting Comments: A NAC solution is important to enable the institution to control the numerous devices connected to the Bank's network, thereby enabling them to identify and protect the network from rogue and compromised devices. The NAC has the ability to discover devices connected to the network and react to them based on preconfigured compliance rules. For example, policies might disallow android devices, or all devices that run Microsoft Windows without the latest service pack or devices without the latest antivirus signature. The use of a NAC device would improve the visibility within the network and enhance the cybersecurity protection of the Bank.

Management Response: CTO Gupta and CISO Tumarinson stated that NAC, to protect the network from unauthorized devices, will be implemented by June 30, 2021.

SR #5-2020 - Change Control

Corrective Action: Management needs to implement a process to detect unauthorized changes within the environment.

Supporting Comments: Discussions with management confirmed that there is no formal process in place to detect changes within in the IT environment that were previously approved in the various change committees and/or by change request systems. IT management confirmed that they are in the process of implementing ServiceNow. However, as of this review there is no definite time for its deployment. Unauthorized changes could be an indication that there is an administrator operating outside of the approved change management process or that there is a breach in the environment.

Management Response: CTO Gupta indicated this will be completed in two phases: 1) The Change Management Module of ServiceNow will be in production by December 31, 2020, and 2) Management will use a risk based approach to identify the systems and applications, and types of changes that will be monitored. Management expects to complete this process no later than September 30, 2021.

EXIT MEETING

An exit meeting was held on June 3, 2020. The Bank was represented by Chairman, President, and CEO Steven Bush, EVP General Counsel Jeffrey Herbert, EVP CTO Debi Gupta, EVP Chief Audit Officer Ronni Silver, EVP CRO Steven Ekert, SVP CISO Max Tumarinson, SVP Enterprise Project

Manager Yana Zimmermann, FVP Deputy Chief Internal Auditor Hillel Judasin, FVP CTO Deputy Anthony Scarola, VP Business Continuity Manager David Camposano, VP Head of Regulatory Relationship and Exams Greisana Muhaj, AVP Regulatory Exam Management Specialist Brendan Corrigan, and AVP Regulatory Exam Specialist Fatima Gillings. Attending from the FDIC was Safety and Soundness (S&S) Onsite Examiner-In-Charge (EIC) Daniel Devlin, S&S Onsite Dedicated Examiner Polenski Sims, Supervisory Examiner (IT) Stephanie Williams, IT EIC Mark Fischer, IT Examiners Wynn Janowitz, Luis Rodriguez, Jennifer Samer, and Georgina Ayenu, with IT Examination Analyst Donald Joyce. S&S Onsite EIC Reena Mathew, Director Cybersecurity Division Mohamed Shehata, Financial Services Examiner Gary Presser and Financial Services Specialist Jeffrey Szarejko represented the NYSDFS. Management was attentive to the findings and recommendations presented.

We request that the Board review this letter at their next meeting and document their review in the minutes of the Board of Directors meeting. Please provide a written response to the outstanding MRBA and to the apparent violation noted in Appendix A within 45 days of the date of this letter. If you have any questions or concerns regarding the content of this letter, please contact FDIC Senior Case Manager Amanda Dubuque at (917) 320-2802 or NYDFS Supervising Bank Examiner Maxine Turner at (212) 709-3837.

Sincerely,

	/S/ Yolanda Ford
Steven P. Slovinski	Yolanda Ford
Assistant Regional Director	Deputy Superintendent of Banks
Federal Deposit Insurance Corporation	New York State Department of Financial Services

cc: Federal Reserve Bank of New York

Appendix A – Violations of Laws and Regulations
Appendix B – Summary of Regulatory Issues

NONCONFORMANCE WITH INTERAGENCY GUIDELINES

The Interagency Guidelines Establishing Information Security Standards (Appendix B to Part 364 of the FDIC Rules and Regulations) establishes certain standards for all insured state, nonmember banks. These standards address the guidelines for developing and implementing administrative, technical, and physical safeguards to protect the confidentiality and integrity of customer information. The institution is in nonconformance with the following sections of Appendix B to Part 364 Safety and Soundness Standards.

Section III C-3 mandates that the bank regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties, or staff independent of those that develop or maintain the security programs.

IT-related risk assessments, including the GLBA risk assessment, continue to need improvement. Descriptions for key risk and controls are brief and do not adequately support inherent risk ratings, control ratings, or residual risk ratings. Risk Assessments should demonstrate sufficient analysis and prioritization of bank-specific risks, and provide an actionable understanding of the key risks in that area. Further, proper independent testing of the key controls should be completed after risk assessments are finalized. Control testing is a valuable tool for identifying and mitigating gaps and supports management in gaining an overall understanding of the risk exposure to existing, expected, or severe events.

Management Response: CRO Steven Eckert is responsible for the establishment of an appropriate GLBA Risk Assessment Framework, and the identification and testing of the key controls. Negotiations have commenced with ITA Partners to assist management with establishing an effective GLBA Risk Assessment, and establishing and testing the key controls. Management plans to have the GLBA Risk Assessment and the identification and testing of the key controls completed by September 30, 2020. The target date to present the GLBA Risk Assessment to the Management Risk Committee and approval by the Board Risk Committee is October 28, 2020.

This section is a brief summary of regulatory findings and recommendations related to Information Technology matters.

Notes on Issue Status:
Open - the issue is open as either management has to take further action or verification of closure needs to occur at the next targeted review.
Closed - the examination process verified that the issue is closed.

Prior Examination - 2016 Summary of Regulatory Issues

Target Area	Issue Description	Issue Type/#	Target Letter	Issue Date	Issue Status
IT- Enterprise Risk Management (ERMP)	Enhance the IT risk assessment program and fully develop the IT risk management framework needed to support the IT-ERMP	MRBA-IT #04/2016	SL #06-2016	10/24/2016	Open
Identification and Documentation of Key Controls	Identify and document the appropriate controls that are in place within the Bank's environment and use for reporting and testing across the three lines of defense.	SR-IT #07/2016	SL #06-2016	10/24/2016	Open

Prior Examination - 2017 Summary of Regulatory Issues:

Target Area	Issue Description	Issue Type/#	Target Letter	Issue Date	Issue Status
Internet Banking System Security Monitoring	Enhance monitoring processes upon conversion with Q2 to include monitoring of anomalous login activities.	SR-IT #15/2017	SL #03-2017	09/07/2017	Closed

Prior Examination - 2018 Summary of Regulatory Issues:

Target Area	Issue Description	Issue Type/#	Target Letter	Issue Date	Issue Status
Inventory and End of Life (EOL) Management	Strengthen oversight over software and hardware inventory. Define a formal process to assess significance of hardware and software to remediate any EOL issues prior to end-of-support date.	SR-IT #0l/2018	SL #04-2018	08/27/2018	Open

Hardening Standards	Develop hardening standards for all infrastructure assets and regularly review the infrastructure for compliance with various build standards to mitigate the risk of attacks.	SR-IT #02/2018	SL #04-2018	08/27/2018	Open
IT Strategic Planning (SP)	Develop an IT SP that includes short- and long-term goals, and the allocation of resources. The IT SP should address budget, periodic Board reporting, and the status of risk management controls. Detailed tactical plans should also be developed to support the IT SP and outline specific steps, personnel, tools and timetables to achieve the IT SP goals.	SR-IT #03/2018	SL #04-2018	08/27/2018	Closed

Prior Examination – 2019 Summary of Regulatory Issues:

Target Area	Issue Description	Issue Type/#	Target Letter	Issue Date	Issue Status
CISO	The CISO should be empowered with sufficient resources and stature to provide effective oversight over the IT Department and the Bank's IS infrastructure.	MRBA-IT #01/2019	SL #06-2019	9/30/2019	Closed
Security Event Monitoring	Management should ensure that all security logs are processed through the Security Information Event Management (SIEM) software and anomalous activity is detected in a timely manner.	SR-IT #01/2019	SL #06-2019	9/30/2019	Open
Encryption Key Management	Encryption key management procedures should be formally documented as required by the Bank's Information Security Policy.	SR-IT #02/2019	SL #06-2019	9/30/2019	Closed

Privileged User Reviews	Conduct detailed entitlement reviews on privileged users for all applications on a quarterly basis. In addition, provide oversight to ensure privileged users of all systems are performed and the depth of the review is adequate.	SR-IT #03/2019	SL #06-2019	9/30/2019	Open
Patch Management	The CISO should provide independent oversight over Patch Management	SR-IT #04/2019	SL #06-2019	9/30/2019	Closed

2020 Summary of Regulatory Issues:

Target Area	Issue Description	Issue Type/#	Target Letter	Issue Date	Issue Status
Network Monitoring	Management should monitor the internal and external network of the bank.	SR-IT #01/2020	SL #03-2020		Open
User Access Rights Administration	Management should implement Role Based Access Control (RBAC).	SR-IT #02/2020	SL #03/2020		Open
Database Management	Management should assess and implement field level logging and monitoring of key databases.	SR-IT #03/2020	SL #03/2020		Open
Network Access Control (NAC)	Management should implement Network Access Control to protect the network from unauthorized devices.	SR-IT #04/2020	SL #03/2020		Open
Change Control	Management should implement a process to detect unauthorized changes within the environment.	SR-IT #05/2020	SL #03/2020		Open