Information Technology RCSA Summary

October 2021

Business Head – Debi Gupta, EVP, CTO
Department Leads/ Team – Anthony Scarola, Allen Lum, Rajesh Kalyanaraman, Jose Mendez, Marie Siegel, Joseph Armenti, Stephen Apruzzese, Franklin Cabral, Joe Petti, Robert Celona, Nicholas Creer, Robert Martin, Michael Lamparello, Jonathan Ruf, Eddie Tsai, Jiahang Lian

Information Technology RCSA Highlights

Information Technology is comprised of several functional teams that provide support to the Business Units. The key processes within Information Technology are: IT Strategy and Governance, IT Development and Acquisition, Change Management, IT Operations, Business Continuity Planning, IT Infrastructure, Data Classification and Encryption ~~and Electronic Banking~~.

Information Technology	Inherent Risk	Control Rating	Residual Risk
I. IT Strategy and Governance	Moderate	Strong	Low
II. IT Development and Acquisition	High	Adequate	Moderate
III. Change Management	High	Adequate	Moderate
IV. IT Operations	High	Strong	Low
V. Business Continuity Planning	High	Adequate	Moderate
VI. IT Infrastructure	High	Adequate	Moderate
VII. Data Classification	High	Adequate	Moderate
VIII. Encryption	High	Adequate	Moderate

Information Technology RCSA Summary

79 key + 9 non-key = 88 in total

6 issues???

Overall, the Information Technology RCSA process has identified 63 key risks across 8 key process areas. There are 81 documented key controls mitigating those risks which were tested. The majority of the risks are rated Low and all of the 9 issues have action plans entered into MetricStream with action plans for remediation.

The Information Technology Risk and Control Self-Assessment (RCSA) was conducted using the Bank's risk management process and approach. The IT RCSA process assesses the risks, control design, and the operating effectiveness of key technology controls. The results were finalized on October 30, 2021. The RCSA resulted in the identification of 9 issues.

Management has developed action plans for the remediation of all identified issues. Key open issues are outlined below and are on track for remediation:

- Implementation of Network Access Control (NAC) and Network Segmentation.
- Completion of discovery and classification of unstructured data.
- Completion of asset catalog, while validating the contents and integrity of related data fields.
- Implementation of a risk-based approach for identifying and managing all unapproved changes to the Bank's information assets to include components of infrastructure, applications and software.
- Finalizing all Business Continuity Plans and non-cyber-related Incident Response Plan.
- Developing and implementing holistic Bank-wide procedures and processes for encryption key management, outside of IT Infrastructure.

Ongoing tracking and monitoring of the open issues is performed via MetricStream.

There are 6 here

I. IT Strategy and Governance – Strengths and Weaknesses

IT Strategy and Governance (Low)

Strengths:

The Bank has implemented a rolling three year plan that incorporates Technology into the Bank's strategic initiatives. The IT Strategic Plan includes projections for both human resources and related investments. The plan is aligned with the Technology Management Framework (TMF), which outlines the corporate strategic objectives. The plan is updated annually and approved by the Board of Directors. The Technology Operations Planning Committee (TOPC) meets monthly to discuss topics such as IT Operations, IT-related regulations, audit findings and self-identified issues. Besides IT management, TOPC includes the CEO and Senior Management from the Business Units, Information Security ("InfoSec"), 2nd line Risk Management, and Internal Audit groups. The InfoSec group reports to the Chief Risk Officer of the Risk Management department, which is independent from IT. Separation of responsibilities is further in place within the IT group, which is organized so that the functions, roles and responsibilities of the teams ensure appropriate segregation of duties. IT and InfoSec Policies are updated and approved by the Board of Directors at least annually. IT develops and maintains a budgeted training program for staff development.

Weaknesses:

There were no significant weaknesses identified.

II. IT Development and Acquisition– Strengths and Weaknesses

IT Development and Acquisition (Moderate)

Strengths:

Information Technology (IT) operationalized a centralized tool (ServiceNow) to provide both automatic and manual methods to track the Bank's IT assets to include hardware and software including business application services, commercial off-the-shelf software and operating systems. An inventory of all physical IT assets was performed in 2020 Q4 and captured within the new ServiceNow centralized Hardware Asset Management (HAM) module. Budget versus actual costs are captured and reviewed as part of the quarterly and annual Technology Operations Planning Committee (TOPC) meetings.

Weaknesses:

IT is on-track to complete the documentation of all assets, while validating the contents and integrity of related ServiceNow inventory data fields. The group is also working with a 3rd party vendor to address a self-identified issue which is that the current version of ServiceNow does not capture the end-of-life (EOL) information on operating systems and some software. In addition, the software does not properly identify/discover information about newly on-boarded applications. Internal Audit identified four issues concerning software licenses of which three have been closed.

III. Change Management– Strengths and Weaknesses

IT Change Management (Moderate)

Strengths:

The Bank has implemented a centralized change management process, using ServiceNow to capture change requests and provide approval through workflows to standardize change procedures, in compliance with the Technology Change Management Policy. All non-standard ("normal" and "emergency") changes must be submitted to, reviewed and approved by the Change Advisory Board (CAB), which meets twice a week with the participation of key stakeholders from business, InfoSec and IT. In addition, with the creation of the ServiceNow asset repository, ownership is now assigned for IT assets to include hardware, software and applications. Through testing we confirmed that changes are appropriately tested and approved prior to deployment. Changes on internally-managed applications/systems are reviewed and approved by the business units.

Weaknesses:

IT is on track to implement a risk-based approach for identifying and managing all unapproved changes to the Bank's information assets, including components of infrastructure, applications and software. Until this is in place, the Bank may be subject to the risks resulting from unauthorized changes not being identified timely and addressed appropriately.

IV. IT Operations – Strengths and Weaknesses

IT Operations (Low)

Strengths:

Servers and applications are backed up locally with encryption. The backup data is replicated offsite for remote storage. Backup testing is performed monthly with results reviewed by management. Database backup and other processing issues are monitored and failures are remediated. Key network components are continuously monitored to include health, routing and resource utilization. The report of the monitoring status is reviewed by the network team for timely response to potential and identified issues. The Bank's data centers are secured by appropriate physical access and environmental controls. In addition to using key-fobs, data center access is controlled by biometrics. There are no significant changes in the core banking system environment (people, process, and technology), and the controls for IT Operations related to this platform continue to be effective in 2021. The Bank is de-converting off this in-house core bank platform to an outsourced platform, so no other changes with the current system are anticipated.

Weaknesses:

In early 2021, during the transition phase from Networker to the Veeam back up solution, testing of the backup restoration were not consistent across applications. In addition, the backup of the Palo Alto firewall environment was being performed manually. Both of these issues are now resolved. There were a number of IT operational risk incidents recorded which were identified and closed during the review. This included outages, and vendor and application-related issues.

V. Business Continuity Planning– Strengths and Weaknesses

Business Continuity Planning (Moderate)

Strengths:

The Business Continuity/Disaster Recovery (BC/DR) team submits and receives approval from Senior Management for a strategy to develop, implement and maintain the bank-wide Business Continuity and Disaster Recovery Programs. The Bank's Business Continuity Plan (BCP) includes individual department-level plans and corresponding Business Impact Analysis (BIA). The BC/DR team facilitates drafting of the Bank-wide Disaster Recovery Plan (DRP). The Pandemic Plan is finalized and a table top exercise of the plan was successfully conducted in 2021. In addition, two exercises were conducted on ransomware by BC Team as well as thein information Security Department. Testing of individual DRP's is also performed to verify the recovery of the McCracken application, the core, and the network environment. The BC/DR Team works with Legal to validate the continuance and appropriateness of insurance policies to cover key and significant cyber-related and non-cyber related risks for unexpected business disruptions. The BCP, DRP, and related documents/information is available from a centrally-located application/repository to ensure the bank's employees, consultants, and vendors can access the same/latest versions of instructions/information when business disruptions occur.

Weaknesses:

The final BCPs and non-cyber-related Incident Response Plan was unavailable for review as the lines of business are scheduled to sign off their individual BCP's at the end of Q1, 2022; and the non-cyber-related Incident Response Plan (IRP) is drafted, due to be released at the end of Q1, 2022. In addition, the BC/DR team is finalizing with Internal Audit a future plan for the IT-centric DRP.

VI. IT Infrastructure – Strengths and Weaknesses

IT Infrastructure (Moderate)

Strengths:

The provisioning of user access to the Bank's infrastructure is now centrally managed by both the IT Service Desk for Active Directory and User Entitlement Group for applications, using the ServiceNow tool. Access to the Bank's infrastructure is required prior to granting access to the Bank's critical applications. Remote access is secured by VPN and further controlled via multi-factor authentication (Okta). Endpoints (servers and workstations) are protected against virus and spyware by CrowdStrike. Patches to operating systems and managed applications are applied regularly via KACE. The Bank's email infrastructure (Gmail, Netskope, and Virtru) protects NPI and PII data, while securing inbound and outbound messages from risks including spam, spoofing, and data loss. Only members of the IT network and server team possess privileged accounts, belonging to a separate Active Directory group, further managed with THYCOTIC, a privileged access management (PAM) solution. Third-Party Service Providers are denied access to systems by default. When granted, access time is limited. Similarly, contractor access to the network is automatically disabled after 90 days. Firewall changes are monitored independently by the Information Security Group. The project to implement "role-based access control" is on schedule, with the business case and project plan submitted and approved by the CEO and TOPC.

Weaknesses:

The Bank is on track to implement Network Access Control (NAC) and Network Segmentation. Until these two initiatives are successfully completed, the Bank may be subject to the risks of being exposed to unauthorized devices or increased attack surface.

VII. Data Classification – Strengths and Weaknesses

Data Classification (Moderate)

Strengths:

The Bank has developed a data classification approach, which includes relevant policies and procedures aligned to the applicable regulatory requirements. Training on the approach and requirements is provided to all Bank employees on an annual basis. The Bank invests in technologies to help automate the process of discovery, identification, and classification of data according to policy. Other tools are implemented to enforce the Bank's data security controls and ensure that they continue to operate effectively. Automated controls and processes are also implemented to prevent unauthorized transmission of data via email and instant messaging. Multi-factor Authentication is further used to secure data access based on risk levels of the platform. To prevent data leaks, a combination of tools and processes are deployed, to include destruction of obsolete equipment potentially containing sensitive data.

Weaknesses:

The Bank is making good progress with its data classification program. While the structured data has been classified, the project plan for implementing tagging of unstructured data (e.g., emails, documents, spreadsheets) will completed by Q2, 2022. There were a number Information Security issues to include regulatory, Internal Audit, and self-identified, which were closed during the review. NYSDFS Part 500 security-related compliance issues are targeted for closure in Q4, 2021.

VIII. Encryption – Strengths and Weaknesses

Encryption (Moderate)

Strengths:

The Bank's policy requires confidential data to be encrypted in transit and at rest, while restricted data is to be encrypted in transit. Most data in the Bank's data center environment is encrypted at rest. In-scope data includes all corporate emails and attachments, inbound and outbound data transmitted over the Internet, and data stored on servers and backup tapes. Several tools and processes are implemented to provide encryption to include VIRTRU for email, BITLOCKER for laptops, and Dell EMC's CloudLink for the encryption of virtual environments (VMware ESXi). Severs that were previously physical/stand-alone (e.g., database, file servers) are now hosted within the Bank's virtual encrypted environment. MISER core backups (VTS) and VEEAM are the tools used to back up and encrypt the data in the Miser System and IT infrastructure respectively. Data at rest is currently under review as part of the data discovery/data classification project to determine the best encryption approach and technology.

Weaknesses:

The processes and procedures for Bank-wide key management are not yet centralized. Currently, key management is limited to the assets under the control of the IT Infrastructure group. There were a number of encryption issues identified through the GLBA assessment and by Internal audit. The internal audit issues were closed during the review period. One GLBA encryption issue remains open is targeted for remediation by year end.

I. 2021 IT Strategy and Governance RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	Moderate	Strong	Low	Stable
2020	Moderate	Strong	Low	N/A

Business Description	~~Apple's~~ Apple Bank's IT Senior Management is responsible for the implementation and management of the IT Strategy and all required governance. This includes the design and implementation control frameworks and supporting IT policies and procedures. Management has developed a Technology Management Framework (TMF), which outlines the corporate strategic objectives. This framework is used to align the IT strategic initiatives with the Bank's strategy and is an ongoing process.
Business Head	**Debi Gupta**
Business Leads	**All Debi Gupta's Direct-Reports**
Business Outlook	The risk trend for this section is stable for 2021. IT Senior Management adapts and updates the Strategic plan, Policies and Procedures at least annually. This ensures an effective management of the increasing investments in technology to meet the Bank's objectives. In the mean time, new initiatives are underway to improve IT compliance and IT control efficiency, in order to ensure the timely delivery of IT value-added services.
Inherent Risk	➢ Overall inherent risk rating is Moderate ➢ Inherent Risk Rating breakdown (3 - Moderate, 3 - Low)
Controls	➢ Majority of controls are rated Strong (8- Strong, 3- Adequate)
Residual Risk	➢ Majority of residual risks are rated Low (6 - Low)

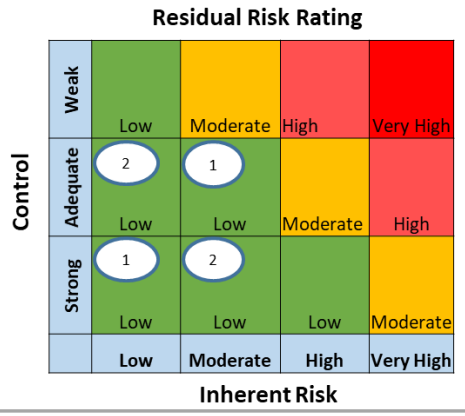
I. 2021 IT Strategy and Governance RCSA

Residual Risk Themes	**Low** Residual Risk themes include: • Updates of IT Policy with changes in applicable regulations and standards • Updates and tracking of IT strategic plan • Definition of IT roles and responsibilities • Monthly TOPC Meeting • Training of IT personnel • IT capital expenditures

Findings/Issues Description	Summary of Action Plans
There are no findings.	There are no action plans.

Key Statistics

- 6 Key Risks Identified
- 11 Mitigating Controls
- 11 Key Controls Tested
- 6 Key Residual Risks – Low



II. 2021 IT Development and Acquisition RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High	Adequate	Moderate	Decreasing
2020	High	Weak	High	N/A

Business Description	The Bank has strengthened its process to record and track IT assets, including: hardware, software, operating systems and applications. This is accomplished by a Bank-wide inventory of all physical assets, a manual cataloging of Business Application Services, and by the implementation of several ServiceNow modules for automatic discovery and tracking of information assets.
Business Head	**Debi Gupta** — **Business Leads**: **Maria Siegel, Anthony Scarola**
Business Outlook	IT continues to validate the asset information to ensure its accuracy and completeness by 2022. This will provide a foundation for an effective and accurate IT asset inventory. IT is assessing the new features in the new version of ServiceNow, which addresses the current issues related to the capture of end-of-life/end-of-support information, and the auto-discovery of new applications.
Inherent Risk	➢ Overall inherent risk rating is High ➢ Inherent Risk Rating breakdown (3- High 1- Moderate)
Controls	➢ Majority of controls are rated Adequate (4- Adequate, 2 - Weak) ➢ Most of the control deficiencies from 2020 have been addressed in 2021 with the implementation of several modules in ServiceNow for automated tracking and discovering IT assets ➢ A physical inventory was conducted to physically tag the assets and enter the information into ServiceNow ➢ Two issues related to the tracking of the operating system's end-of-life (EOL) and the auto-discovery of assets have been identified. These issues are expected to be remediated with the new version of ServiceNow.
Residual Risk	➢ Majority of residual risks are rated High (2 – High, 1 – Moderate, 1 - Low). ➢ The aggregate residual risk is Moderate based upon the Control Grid ??.

II. 2021 IT Development and Acquisition RCSA

Residual Risk Themes	**High** Residual Risk themes include: • Inventory of IT assets (hardware, software, applications, etc.) may not be appropriately and accurately accounted • Upgrade of End of life and end of Support for IT Assets **Moderate** Residual Risk themes include: • IT Asset Management Process **Low** Residual Risk themes include: • Management of budgeted versus actual IT expenditures

Findings/Issues Description

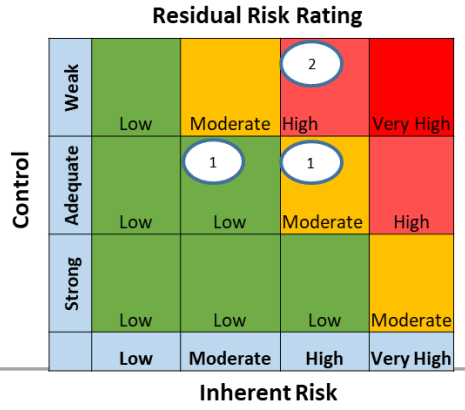
- Key fields data fields need to be fully validated and correctly populated with accurate data.
- The current version of Service Now does not allow the capturing of EOL data from OS Software.
- ServiceNow CMDB does not pick up (discover) the applications properly.

Summary of Action Plans

- Continue the process of updating and validating IT Software Asset Inventory. Target Date: 03/31/22.
- Upgrade to new version of Service Now. Target Date: 12/31/20221.

Key Statistics

- 4 Key Risks Identified
- 6 Mitigating Controls
- 6 Key Controls Tested
- 2 Key Residual Risk – High
- 1 Key Residual Risk – Moderate
- 1 Key Residual Risks – Low



III. 2021 Change Management RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High (*)	Adequate	Moderate	Decreasing
2020	Very High	Adequate	High	N/A

Business Description

IT Change Management has a high inherent risk, which is in line with the industry. The IT change Management Policy is now in place as well as the necessary IT change management procedures to ensure a successful Change Management process.

Business Head | **Debi Gupta** | **Business Leads** | **All Debi Gupta's Direct-Reports**

Business Outlook

The risk trend in this section is decreasing as the Bank is centralizing its IT change operations within ServiceNow. The Bank automates its change processes with the ServiceNow workflow capability, archives all the artifacts related to the changes in the ServiceNow change repository, and documents its information assets (infrastructure components, applications and software) using ServiceNow asset management technology.

Inherent Risk

- Overall inherent risk rating is High (*)
- Inherent Risk Rating breakdown
  (1 - Very High, 7 - High, 3 - Moderate)

Controls

- Majority of controls are rated Adequate (2 - Strong, 10- Adequate, 1 - Weak)
- Many controls are semi-automated thanks to the implementation of ServiceNow workflow in order to enforce the IT change management policy and to simplify routine procedures (e.g., "standard change")
- All the controls are fully tested, except one control that is related to the ongoing initiative for automated change monitoring
- Six action plans were established during last year's RCSA to centralize and automate the change management process. These were addressed adequately with the implementation of ServiceNow.
- There were eight (8) change management-related incidents in 2021, caused by the failure in the Bank's internal controls . In addition, there was one (1) incident related to the failure in the vendors' internal controls.

Residual Risk

- Majority of residual risks are rated Moderate (2 - High, 6 - Moderate, 3 - Low).
- All the processes are automated to the extent it is possible to integrate them with the ServiceNow workflow. Some processes remain reliant to the human intervention such as change approval and user acceptance testing.

(*) See Appendix 1- 1.1

III. 2021 Change Management RCSA

Residual Risk Themes

High Residual Risk themes include:
- Implementation of unauthorized change
- Detection and monitoring of unauthorized change

Moderate Residual Risk themes include:
- Enforcement of IT Change Policy
- Improper categorization of change
- Independent review of change post-implementation
- User acceptance test
- Change communication
- Change logging and tracking

Low Residual Risk themes include:
- Change evaluation
- Back out plan
- Change reporting

Findings/Issues Description

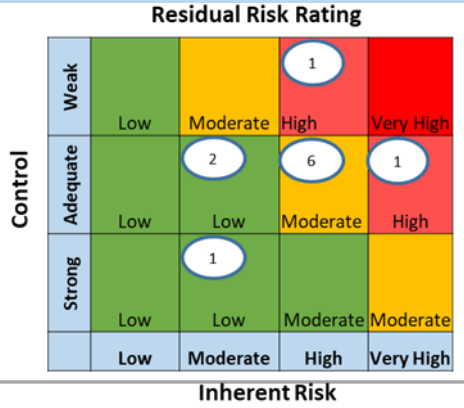
Management needs to implement a process to detect unauthorized changes within the environment. This is an existing [Regulatory] finding.

Summary of Action Plans

- The Change Management Module of ServiceNow will be in production. Target Date: December 31, 2020. (Completed)
- Management will use a risk based approach to identify the systems and applications, and types of changes that will be monitored. Target Date: December 30, 2021.

Key Statistics

- 11 Key Risks Identified
- 13 Mitigating Controls
- 10 Key Controls Tested (3 Non Key also tested)
- 2 Key Residual Risks – High
- 6 Key Residual Risks – Moderate
- 3 Key Residual Risks – Low



III. 2021 Change Management RCSA

Change Management-related Incidents

Incidents due to failure in internal controls within Apple Bank

• "WirePro & BSA Manager SSL Implementation": due to lack of development testing	ISSUE-0000001485	Closed
• "eWire Transfer Posting": due to a configuration error that connected the eWire testing environment to the Miser production	ISSUE-0000003097	Closed
• "WirePro Production issues - Application Inaccessible": due to the errors when updating the TLS protocol in accordance with CIS Standards	ISSUE-0000001440	Closed
• "Auto-notifications of data movement sent externally in error": due to a configuration error	ISSUE-0000003106	Closed
• "Applebank.com DNS connectivity issue" : due to a configuration error	ISSUE-0000003374	Closed
• "Gmail Outage in Chanin": due to firewall rule update	ISSUE-0000003326	Closed
• PILOT PROGAM TESTING: Calls Not Recorded due to internal Firewall Update	ISSUE-0000003430	New
• "Email encrypted by error": due to a Virtru test rule erroneously applied to all users	ISSUE-0000003400	Pending Review

Incidents due to failure in internal controls within Apple Bank's vendors

• "BAM+ Data Manager Module Incorrect Access": due to errors in vendor's new release	ISSUE-0000003424	Closed

IV. 2021 IT Operations RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High	Strong	Low (*)	Stable
2020	High	Strong	Moderate (*)	N/A

Business Description

IT Operations has a High inherent risk, which is in-line with the industry. Key areas such as backup and recovery, overnight job processing and monitoring, infrastructure monitoring and physical access are automated aggressively in 2021 to allow the Bank to lower the risks in this area and improve its efficiency.

Business Head | **Debi Gupta** | **Business Leads** | **All Debi Gupta's Direct-Reports**

Business Outlook

The risk trend in this section is stable as the Bank further automates its operations with technologies to include Veeam and Iron Mountain cloud (backup), SolarWinds (infrastructure monitoring), and SQL Server technology (data-related overnight jobs). Over the next two years the Bank is de-converting off of the current in-house core banking platform to an outsourced platform, and as a result, no further changes are anticipated.

Inherent Risk

- Overall inherent risk rating is High
- Inherent Risk Rating breakdown
  (4 - High, 4 - Moderate)

Controls

- Majority of controls are rated Strong (11 - Strong, 3 - Adequate)
- Most controls are automated, which lowers the risk, increases the efficiency and effectiveness of the operations
- All controls were fully tested, except those related to MISER which did not experience any significant changes in anticipation of future replacement, and those related to the environment which were re-classified as non-key.
- Some incidents are registered in MetricStream that may be related to IT Operations. These incidents are closed or in the process of being closed, with low chance for re-occurrence.
- There were sixteen (16) IT operations-related incidents in 2021, caused by the failure in the Bank's internal controls. In addition, there were six (6) incidents related to the failure in the vendors' internal controls.

Residual Risk

- Majority of residual risks are rated Low (1 - Moderate, 7 - Low), aggregate residual risk assessed as Low.
- All key processes are automated with technology such as Veeam and Iron Mountain cloud backup, SolarWinds (infrastructure monitoring), and SQL Server technology (data-related overnight jobs).

(*) Risk scoring methodology has changed from 2020 which accounts for the Low residual risk in 2021.

IV. 2021 IT Operations RCSA

Residual Risk Themes

Moderate Residual Risk themes include:
- Management of data center physical access

Low Residual Risk themes include:
- Back up of applications and infrastructure
- Independent review of physical access
- Maintenance of data center environmental controls
- Management of business application reports
- Monitoring of system resource and system performance
- Report of performance metrics
- Automated scheduling of jobs (in-house managed systems)

Findings/Issues Description

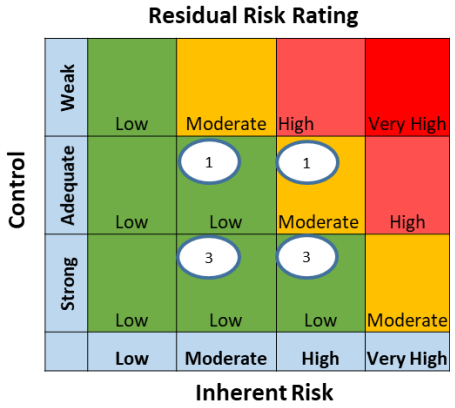
There are no findings.

Summary of Action Plans

There are no outstanding action plans.

Key Statistics

- 8 Key Risks Identified
- 14 Mitigating Controls
- 13 Key Controls Tested (1 Non Key tested)
- 1 Key Residual Risks - Moderate
- 7 Key Residual Risks – Low



III. 2021 IT Operations RCSA

IT Operations-related Incidents

Incidents due to failures in internal controls within Apple Bank

• "Back up Tapes for the virtualized servers in Scarsdale were not usable": Uncovered, while performing an exercise on system restoration.	ISSUE-0000000190	Closed
• "FCC Table Replication Issue": due to a status change on wires.	ISSUE-0000000191	Closed
• "Solarwinds Change Reports not distributed": reports not stored on the server due to insufficiently specified retention period	ISSUE-0000001484	Closed
• "Q2 Online Banking/MB banking & Miser degradation of service": due to database running out of space	ISSUE-0000001442	Closed
• "Q2 OLB - CentrixDTS - Encryption Keys Stored in Plain Text"	ISSUE-0000001368	Closed
• "Q2 Online Banking/MB banking Centrix degradation"	ISSUE-0000003429	Closed
• "Unable to run the BSA Manager's nightly daemon"	ISSUE-0000001634	Closed
• "VMWare Horizon was not accessible"	ISSUE-0000001635	Closed
• "Deleted Abrigo BAM+ and WirePro Wires": 11,031 wires were marked as deleted in the SQL database	ISSUE-0000001636	Closed
• "McCracken System Outage": due to omission of restarting a connecting device	ISSUE-0000001642	Closed
• "FedLine Application outage": due to loss of Internet access from Spectrum	ISSUE-0000003083	Open
• "Miser Date Roll/ Update Incident": Timing error after system shut down for back up	ISSUE-0000003115	Closed
• "WirePro Branch Wire Entry Issue": Unable to send wires.	ISSUE-0000003236	Closed
• "Network access outage": due to VMware storage degradation	ISSUE-0000003373	Closed
• "S1 Connectivity outage": due to duplicate MAC address.	ISSUE-0000003422	Closed
• "Chanin Gmail outage": due to the disabling of a firewall rule (change authorized per CHG0030540)	ISSUE-0000003078	Closed

III. 2021 IT Operations RCSA

IT Operations-related Incidents

Incidents due to failures in internal controls within Apple Bank's vendors

• "Devices Offline in Chanin": due to broadcast storm	ISSUE-0000003327	Closed
• "Branch 29 Outage": due to vendor dislodging a branch router plug by error	ISSUE-0000003328	Closed
• "Centrix Application failed to communicate to Mainframe": due to vendor error	ISSUE-0000003395	Closed
• "(PILOT PROGRAM TESTING) Calls Not Recording via Calabrio": due to vendor error	ISSUE-0000003402	Closed
• "FCC - Sanctions Corrupted File": due to a corrupted data provided by Abrigo	ISSUE-0000000192	Closed
• "Okta Portal Disruption": due to Okta system outage	ISSUE-0000003310	Closed

V. 2021 Business Continuity Planning RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High (*)	Adequate	Moderate	Decreasing
2020	Very High	Weak	Very High	N/A

Business Description	IT Business Continuity has a high inherent risk, which is in line with the industry. The Bank's lines of business are owners of the business continuity plans and the related business impact analyses to ensure that the analyses reflect the true nature of the Bank's operations, which would be relied upon for the recovery in the case of business disruptions.
Business Head	**Debi Gupta** — **Business Leads**: **David James**
Business Outlook	The risk trend in this section is decreasing as the Bank is making good progress to put in place not only the Business Continuity Plan, the Pandemic Plan, and the Disaster Recovery Plans, but also a robust process to test the plans, to communicate them to employees and contractors, and to update them whenever there are major changes to the Bank's business, operations, people, and/or technology.
Inherent Risk	➢ Overall inherent risk rating is High (*) ➢ Inherent Risk Rating breakdown (7 - High, 1 - Moderate)
Controls	➢ Majority of controls are rated Adequate (9- Adequate, 4 - Weak) ➢ Most controls are manual, because they are related to planning and testing ➢ Certain controls could not be fully tested because RCSA was conducted before the completion of the related activities. In addition, not available for testing are the disaster recovery plan (available as soon as the cloud strategy is finalized) and the non-cyber related incident response plan (due by the end of 2021) ➢ An action plan is discussed with Internal Audit to remediate the lack of a bank wide disaster recovery plan
Residual Risk	➢ Majority of residual risks are rated Moderate (2 – High, 5 – Moderate, 1 - Low). ➢ The lines of business are taking ownership of their individual business continuity plans and business impact analyses to ensure that they accurately reflect the risk and impact to the businesses at the Bank.

(*) See Appendix 1-1.2

V. 2021 Business Continuity Planning RCSA

Residual Risk Themes

High Residual Risk themes include:
- Completion of disaster recovery plan
- Completion of non-cyber related incident response plan

Moderate Residual Risk themes include:
- Planning and Preparation of business continuity/disaster recovery programs
- Completion of Business Impact Analysis
- Testing of Pandemic Plan
- Testing of business continuity/disaster recovery plans
- Reporting of business continuity/disaster recovery program status

Low Residual Risk themes include:
- Coverage of business interruption insurance

Findings/Issues Description

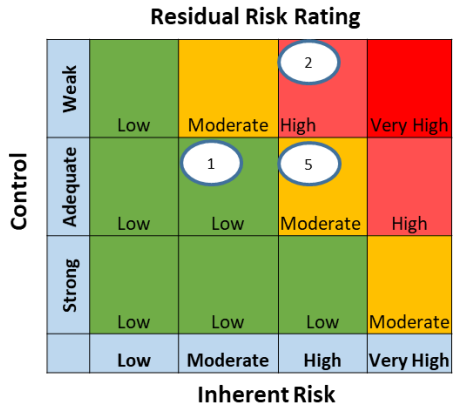
The BCP's and BIA's are not reviewed and signed off. The Bank-wide DRP is not available.

Summary of Action Plans

The lines of business are targeting to sign off their plans. Target Date: 3/31/2021.

Key Statistics

- 8 Key Risks Identified
- 13 Mitigating Controls
- 13 Key Controls Tested
- 2 Key Residual Risks – High
- 5 Key Residual Risks – Moderate
- 1 Key Residual Risk – Low



VI. 2021 IT Infrastructure RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High	Adequate	Moderate (**)	Stable
2020	High	Strong (*)	Moderate (**)	N/A

Business Description	IT Infrastructure has a high inherent risk, which is in line with the industry. Key areas such as access provisioning, network access monitoring, network segmentation, and single sign-on will be enhanced over the year to allow the Bank to improve its infrastructure security posture.
Business Head	**Debi Gupta**
Business Leads	**Jose Mendez**
Business Outlook	The risk trend in this section is stable as the Bank will prepare a business case and a formal proposal to centralize access management and role-based access for all applicable applications that will be reviewed by senior management for deployment. Additionally, the Bank will implement a Network Access Control (NAC), is simultaneously implementing a DMZ, and is executing a plan for network segmentation, currently underway.
Inherent Risk	➢ Overall inherent risk rating is High ➢ Inherent Risk Rating breakdown (3 - Very High, 3 - High, 2 - Moderate, 3 - Low)
Controls	➢ Majority of controls are rated Adequate because there are two weak control (7 - Strong, 7- Adequate, 2 - Weak) ➢ Most controls are automated, which lowers the risk, increases the efficiency and effectiveness of the infrastructure-related controls ➢ All controls were fully tested ➢ Two deficiencies are found: network access control (NAC) and network segmentation. Both are outstanding issues from RCSA 2020. Both have related action plans, which are in progress. (*) In 2020 there were 23 controls tested – (12 Strong, 5 Adequate, 6 weak) with the aggregate rating assigned as Strong. In 2021 there were 16 controls tested and 7 controls were moved to IT Operations. IT remediated 4 out of 6 weak controls in 2021. Therefore the 2021 testing resulted in a rating of 7 Strong, 7 Adequate and 2 weak. The aggregate rating assigned is Adequate.
Residual Risk	➢ Majority of residual risks are rated Low (2 – Very High, 1 – High, 1 – Moderate, 7 - Low) with the aggregate score as Moderate. ** Risk scoring Methodology has changed from 2020 which accounts for the Moderate Residual Risk in 2021.

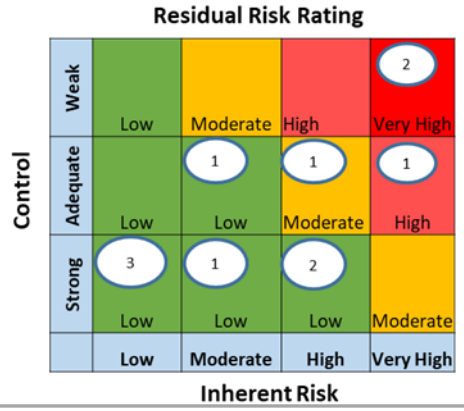
VI. 2021 IT Infrastructure RCSA

Residual Risk Themes	
	Very High Residual Risk themes include: • Implementation of Network Access Control • Implementation of Network segmentation **High** Residual Risk themes include: • Implementation of Role based access **Moderate** Residual Risk themes include: • Access to firewall and reconciliation of firewall changes **Low** Residual Risk themes include: • Management of network privilege access • Implementation of single sign on • Management of IT vendor • Management of service provider access • Implementation of remote access • Protection against virus and malware • Management of patches

Findings/Issues Description	Summary of Action Plans
Network Access Control (NAC) and Network Segmentation are not yet completed.	Management expects to complete both projects (NAC and Network Segmentation). Target Dates: 10/31/2021 and 11/30/21, respectively.

Key Statistics

- 11 Key Risks Identified
- 16 Mitigating Controls
- 15 Key Controls Tested (1 Non Key)
- 2 Key Residual Risks – Very High
- 1 Key Residual Risks – High
- 1 Key Residual Risks – Moderate
- 7 Key Residual Risks – Low



VII. 2021 Data Classification RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High	Adequate	Moderate	N/A
2020 (*)	N/A	N/A	N/A	N/A

Business Description	Data classification has a high inherent risk, which is in line with the industry. It is vital for the Bank to determine the value of its information assets as well as the risks that these assets are exposed to. The value of the information assets and their related potential risks can be assessed once the assets are identified, then classified according to their importance to the Bank's operations as well as their requirement for confidentiality, integrity and reliability. A number of tools have been implemented to automate the key areas such as data discovery, monitoring and protection.
Business Head	**Max Tumarinson** — **Business Leads**: **Jonathan Ruf**
Business Outlook	The residual risk in this area is Moderate, as the Bank has made significant progress in the last year. The project to complete the data classification in on track for completion by Q2, 2022. In the meantime, the Bank adopts the policy to encrypt confidential and restricted data, and is encrypting most data within the Bank's data center environment.
Inherent Risk	➢ Overall inherent risk rating is High ➢ Inherent Risk Rating breakdown (8 - High, 2 - Moderate)
Controls	➢ Majority of controls are rated Adequate (8 - Adequate, 2 - Weak) ➢ A completed data classification of unstructured data has not been performed. The project plan is expected to be developed by Q2, 2022 ➢ To mitigate the risk of incomplete data classification, the Bank requires that all data, both in transit and at rest, be encrypted
Residual Risk	➢ Majority of residual risks are rated Moderate (2 - High, 6 - Moderate, 2 - Low).

(*) An RCSA was not conducted for this area in 2020.

VII. 2021 Data Classification RCSA

Residual Risk Themes

High Residual Risk Themes include:
- Data Classification Process - Misclassification of critical data elements
- Data Discovery Program – Unauthorized access and/or disclosure of data due to improper classification and protection

Moderate Residual Risk themes include:
- Access Controls and IAM Program – Lack of controls over access to critical data
- Monitoring Program - Improper detection of data protection issues due to use of incorrect tools
- Network Controls Processes – Improper transmission of confidential data
- Encryption Processes - Transmitting confidential data in clear text
- Data Protection and Access Controls – Unauthorized disclosure of confidential data
- DLP Monitoring Processes – Confidential Data – Unauthorized disclosure of data

Low Residual Risk themes include:
- Training on Data Classification Policies - Incorrect application of data classification standards
- Removal / Destruction of Expired Data / Devices - Unauthorized disclosure or use of data which is not removed on a timely basis

Findings/Issues Description

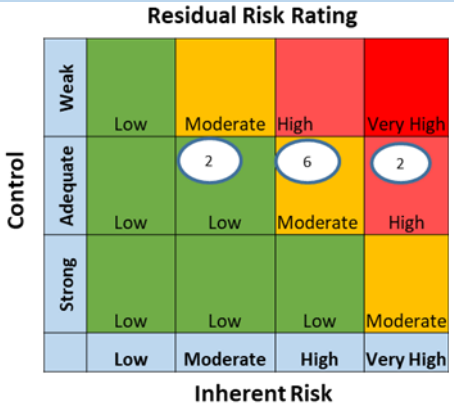
Discovery and labeling of unstructured data needs to be performed in accordance with the Data Classification Policy.

Summary of Action Plans

A project plan will be completed for the discovery and labeling of unstructured data. Target date: 6/30/2022.

Key Statistics

- 10 Key Risks Identified
- 10 Mitigating Controls
- 10 Key Controls Tested (0 Non Key)
- 2 Key Residual Risks – High
- 6 Key Residual Risks – Moderate
- 2 Key Residual Risks – Low



VIII. 2021 Encryption RCSA

RCSA Year	Inherent Risk	Control Rating	Residual Risk	Risk Trend
2021	High	Adequate	Moderate	N/A
2020 (*)	N/A	N/A	N/A	N/A

Business Description	The Encryption domain has a High inherent risk, which is in-line with the industry. The Bank's encryption policy requires confidential and restricted data to be encrypted; confidential encrypted at rest/in transit, and restricted encrypted at rest. The Bank invests in technology and processes to ensure industry-standards and to secure the encryption keys across key assets, including corporate emails, inbound and outbound web traffic, servers and associated data files, as well as offsite backup tapes.

Business Head	**Max Tumarinson**	**Business Leads**	**Jonathan Ruf**

Business Outlook	The residual risk is Moderate. A program will be completed by the second quarter 2022 to ensure that all unstructured and outlier data be discovered, identified, and properly classified; to confirm the Bank's Data Classification and Encryption Policies are being complied with.
Inherent Risk	➢ Overall inherent risk rating is High ➢ Inherent Risk Rating breakdown (3 - High, 2 - Moderate)
Controls	➢ Majority of controls are rated Adequate (4 – Adequate, 1- Weak) ➢ All of the controls are preventive controls with the objectives to protect data against unauthorized disclosure. ➢ The encryption methods are reviewed annually to ensure that the related technologies and methods are up to date to address potentially new threats. ➢ Full disk encryption is currently implemented for all physical and virtual technology assets. ➢ The Bank is implementing a key management technology to manage the encryption keys. An action plan is established to conclude the project by Q2, 2022.
Residual Risk	➢ Majority of residual risks are rated Moderate (1- High, 2 - Moderate, 2 - Low)

(*) An RCSA was not conducted for this area in 2020.

VIII. 2021 Encryption RCSA

Residual Risk Themes

High Residual Risk themes include:
- Key Management - Lack of control over encryption keys may result in compromise of confidential data

Moderate Residual Risk themes include:
- Enterprise Wide Encryption Processes - Unauthorized access to sensitive information on systems and applications due to weak encryption
- Encryption Strength – Compromise and disclosure of data due to weak encryption keys

Low Residual Risk themes include:
- Security Application Risk Review Processes - Unauthorized disclosure of sensitive information due to weak encryption
- IT Infrastructure - Unauthorized access to encryption keys may result in compromise of confidential data

Findings/Issues Description

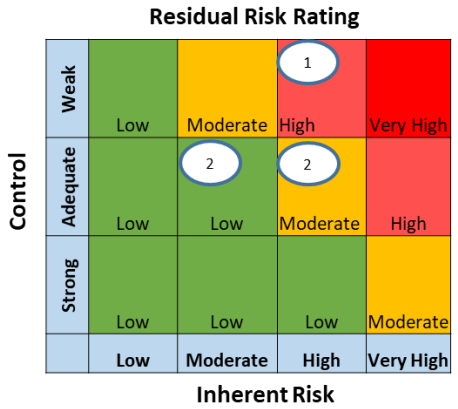
Development of a centralized process and procedures are necessary for key management that will accommodate various applications and devices within the Bank's environment.

Summary of Action Plans

Software for key management is being evaluated and once it has been identified, a project plan will be put in place for implementation. Target Date: 12/31/2021.

Key Statistics

- 5 Key Risks Identified
- 5 Mitigating Controls
- 3 Key Controls Tested (2 Non Key also tested)
- 1 Key Residual Risks – High
- 2 Key Residual Risks – Moderate
- 2 Key Residual Risks – Low



Key Residual Risks Detail

I. IT Strategy and Governance - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
IT Strategic Planning Process	Moderate	The Information Technology Group ("IT") may misalign its activities and priorities against the Bank's strategic objectives because the IT strategic planning is not adequately managed and communicated. This may result in IT being unable to adequately support the Bank's priorities and objectives.	Strong	The Bank has implemented a multiyear plan that incorporates IT into the Strategic Initiatives. This plan includes strategy and projections for both human resources and related investments The plan is aligned with the Technology Management Frame Work (TMF), which outlines the corporate strategic objectives. The Plan is reviewed and approved by the board of directors. The monthly TOPC meeting includes the CEO and Senior Management from the Information Technology ("IT") group. Topics such as IT operations, IT-related regulations and audit findings are discussed.	N/A	N/A	N/A

I. IT Strategy and Governance - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
IT Organization Business Units/ Functions	Moderate	The effectiveness of the design and operating of the technology-related controls at the Bank may not be assured because there is no clear segregation of duties in the roles and responsibilities within the Information Technology ("IT") group and the Information Security ("InfoSec") group. This may create an insecure operational environment that results in severely negative impacts to the Bank.	Strong	The Information Technology Group has been set up to ensure that appropriated segregation of duties is in place as certain IT functions should be separated. The information security ("InfoSec") group reports to the Chief Risk Officer of the Risk Management department, which is independent from the Information Technology ("IT") group. Each position in the Information Technology ("IT") group has a corresponding description of the roles and responsibilities within IT and the Bank	N/A	N/A	N/A
Information Technology Committee	Low	Critical IT activities are not appropriately and timely coordinated because there is no regular meeting within the Information Technology ("IT") group. This may result in IT being unable to adequately support the Bank's priorities and objectives.	Strong	The Information Technology ("IT") group holds a biweekly meeting to discuss IT-related priorities and issues. The CTO meets with the IT Managers to ensure that there is adequate and timely coordination and communication within IT.	N/A	N/A	N/A

I. IT Strategy and Governance - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Information Technology Policy and Procedures	Moderate	The governance of the Information Technology ("IT") group may not be effective because the IT Policies and procedures are not adequately and timely developed, updated and approved. In addition, the policies may not align to the Bank's higher level policies or regulatory requirements. This may result in IT being unable to adequately support the Bank's priorities and objectives.	Adequate	The Bank develops, updates and approves the appropriate Information Technology ("IT") policies and procedures to provide guidance and monitor the IT activities and its consumption. These policies are in alignment with the Bank's higher level policies and the applicable regulatory requirements.	N/A	N/A	N/A
IT and IS Staff Training	Low	The performance of the Information Technology ("IT") group may be negative impacted because the IT staff do not receive appropriate and timely training that is necessary for their roles and responsibilities. This may result in IT being unable to adequately support the Bank's priorities and objectives.	Adequate	The Information Technology ("IT") group develops and maintains a training program for the IT staff to maintain and develop their skill sets. The training program is adequately budgeted each year.	N/A	N/A	N/A

I. IT Strategy and Governance - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Capital Expenditures	Low	The Information Technology Assets may not be appropriately accounted for because the process to manage and report the IT-related capital expenditures and operating expenses is not appropriately defined and maintained. This may result in the Bank wasting human, financial and technical resources and missing strategic opportunities.	Adequate	The Information Technology ("IT") group develops and maintains a process to manage and report the IT-related capital expenditures and operating expenses.	N/A	N/A	N/A

II. IT Development and Acquisition - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Inventory of IT Asset and Business Software	High	The Bank's IT assets (hardware, software, applications, etc.) may not be appropriately and accurately accounted for because the IT Asset Management (ITAM) process is not adequate. This may result in inefficient and deficient support, deployment, maintenance, upgrade, and disposal of IT assets.	Weak	Management establishes an IT Asset Management (ITAM) process to manage the lifecycle of both hardware and software assets. To the extent that is practicable, the ITAM process is automated and integrated with other ancillary data sources at the Bank, such as the asset inventory in the Balance Sheet and the asset-related data from IT Help Desk. A Physical Inventory of IT Assets are taken on a periodic basis (every 1 -3 years) and reconciled to the assets records in Service Now	In summary, the team is still in the process of gathering, obtaining and validating information to complete the IT Asset Inventory. We recommend that continued emphasis to be placed on validating the IT Assets Information in Service Now. In addition, we recommend that a Holistic review be performed to further determine which additional fields should be candidates for further population, such as: Asset Cost, Acquisition date, etc.	IT will continue to validate the hardware asset information in Service Now. IT will work with Accounting dept. to determine if there is any value in recording asset cost.	3/31/2022

II. IT Development and Acquisition - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Software OS Inventory	High	IT assets may no longer function or be adequately supported by suppliers/vendors because the assets have reached the status End-of-Life (EOL) or End-of-Support (EOS). This may expose the Bank to potential business disruptions or security risks.	Weak	IT Asset inventory processes must capture the vendor's End of Life and End of Support dates for purposes of replacement/disposal planning and risk management.	Continue the process of updating and validating IT Software Asset Inventory. Perform a second holistic look to examine whether there should be additional fields that could facilitate future integration with PeopleSoft. The additional field candidates include: Actual costs per Unit, Retirement date, software licenses numbers, etc.	IT will continue the process of updating and validating IT Software/Hardware Asset Inventory. *(There is a related Audit issue and a Self-Identified Issue)*	3/31/2022

II. IT Development and Acquisition - Key Residual Risks – Moderate/ Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Application Inventory *(Moderate Residual Risk)*	High	IT assets may no longer be adequately supported by suppliers/vendors because vendor-related changes are not adequately monitored. This may expose the Bank to potential business disruptions or security risks.	Adequate	Management Maintains an Inventory of Applications so that there is a process in place to ensure that each is supported by the vendor. End-of-life and end-of-support IT assets are timely reviewed so that upgrades or alternatives to upgrades can be put in place in time.	N/A	N/A	N/A
Budget Vs Actual Management *(Low Residual Risk)*	Moderate	Expenses related to IT assets may not be appropriately controlled because the monitoring of these expenses as well as the planning, budgeting, and acquisition of IT assets are not adequate. This results in inefficient usage of the Bank's financial resources.	Adequate	Reports are generated from the Finance Group which are used by the CTO to monitor ongoing expenses. Technology Management will analyze usage and other data to make cost-effective decisions and inform IT resource planning, budgeting, and future acquisitions.	N/A	N/A	N/A

III. Change Management - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	Very High	An unauthorized change may be made to the Bank's operating environment, because the Bank's Change Management Policy and Procedures are inadequately enforced. This may result in negative operational performance, as well as adverse regulatory and financial impacts to the Bank.	Adequate	Changes to technology assets must have a change requestor, who possesses critical domain knowledge related to that request. The change requestor submits the change request, ensures that the request meets the requirements of the Change Management policy and that the request is reviewed by the appropriate manager(s), if applicable. Changes to a business application must be requested by or in agreement with the business owner of that business application.	N/A	N/A	N/A

III. Change Management - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	High	An unauthorized change to the Bank's operating environment may not be identified timely and appropriately, due to ineffective monitoring. This may result in adverse operational effects to the Bank.	Weak	All key and mission critical technology assets (infrastructure, software, applications, etc.) are monitored for changes. The monitoring result is reviewed frequently to identify unauthorized changes. 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. The unauthorized changes are addressed timely and appropriately.	Management needs to implement a process to detect unauthorized changes within the environment. *(existing issue and action plan from the FDIC)*	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 December 30, 2021.	12/31/20 Completed 12/30/21

III. Change Management - Key Residual Risks – Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	High	The potential risks related to the change to a technology asset may not be inadequately assessed, because the asset owner has incorrectly categorized the change. This may result in adverse operational effects to the Bank.	Adequate	Application Owner evaluates the proposed change to determine applicability	N/A	N/A	N/A
	High	A change to a technology asset may not be appropriate, because it has not been approved before the deployment of the change by the appropriate authority. This may result in adverse operational effects to the Bank.	Adequate	Proposed changes to a technology asset (infrastructure, application, etc.) are approved by the designated owner of the asset before the changes are deployed to production	N/A	N/A	N/A
	High	Key operational areas that are affected by a change may not be tested, because the changes have not been subject to independent review. This may result in adverse operational effects to the Bank.	Adequate	Independent review of a change to a technology asset (infrastructure, application, etc.) is performed to determine if all stakeholders are involved in the decision making and testing of the change.	N/A	N/A	N/A

III. Change Management - Key Residual Risks – Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	High	Key operational areas that are affected by a change may not be tested, because the changes have not been subject to a user acceptance test. This may result in adverse operational effects to the Bank.	Adequate	User acceptance testing is performed to ensure that the stakeholders are comfortable with both the changes and risks.	N/A	N/A	N/A
	High	A change to a technology asset may not be appropriate, because it has not been communicated so that the asset stakeholders can help assess the potential risks to the Bank operations. This may result in adverse operational effects to the Bank.	Adequate	Stakeholders to the technology asset (infrastructure, application, etc.) are informed of the change prior to implementation.	N/A	N/A	N/A

III. Change Management - Key Residual Risks – Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	High	Investigation of a change to a technology asset may not be possible, because the change is not properly logged and tracked. This may hamper the effort to recover and restore from disruption, leading to potentially adverse operational effects to the Bank.	Adequate	Changes that are deployed to the production environment are logged and tracked. The implementation steps are documented when appropriate and the implementation status recorded. Compliance with the change management policy and procedures is ensured before closing the changes.	N/A	N/A	N/A

III. Change Management - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	Moderate	A change to a technology asset may not be appropriate, because the risks related to the change have not been evaluated from the perspectives of both business and technology. This may result in adverse operational effects to the Bank.	Adequate	Proposed changes to a technology asset (infrastructure, application, etc.) are assessed by both Technology and Business to determine whether the changes can negatively impact the business operations and whether the changes are compatible to the Bank's technology infrastructure. In addition, changes to a technology asset with direct impact to a business function are reviewed by the designated owner of the business function when applicable. Evidence of this process is attached to the change ticket.	N/A	N/A	N/A

III. Change Management - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Change Management	Moderate	A change may not be appropriate to the Bank, because it has not been reported to the Bank's senior management. This may result in adverse operational effects to the Bank.	Strong	All normal and emergency changes of high-significance are reported to the Technology Operations Planning Committee ("TOPC") on a monthly basis. Changes related to New Products and Initiatives Committee ("NPIC") activities are reported to the NPIC.	N/A	N/A	N/A
	Moderate	A change that contains errors cannot be reverted, because there is no back-out plan. This may result in adverse operational effects to the Bank. (proposed new risk statement)	Adequate	A back-out option exists so that the production environment can be reverted to its stabile conditions prior to changes, should the changes exhibit adverse effects to the processing environment.	N/A	N/A	N/A

IV. IT Operations - Key Residual Risks – Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Data Center Physical Access	High	The security of the Data center and Computer rooms may be compromised because the physical access to these premises are inadequately and inappropriately granted. This may expose the Bank to adverse financial, operational and regulatory issues.	Adequate	Physical access to the Data Center and Computer Rooms is approved by the CTO. Bank Security Officer/Head of Physical Security and CTO review access reports. Physical access is secured with key fobs and multi-factor authentication (MFA) that are controlled by the Bank Security Officer/Head of Physical Security.	N/A	N/A	N/A

IV. IT Operations - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Data Center Environmental Controls	High	Servers and other hardware components in the data center and computer rooms may fail to operate as expected because the data center and computer rooms are not appropriately protected from the environmental risks. This may cause unexpected business interruptions and expose the Bank to adverse financial, operational and regulatory risk and issues.	Strong	The Scarsdale and Chanin Data Center are adequately protected by the appropriate environment controls.	N/A	N/A	N/A
Independent Physical Access Reviews	Moderate	Physical access to the data center and computer rooms may be inappropriate because it has not been regularly reviewed. This may expose the Bank to adverse financial, operational and regulatory risks and issues.	Strong	Physical Access to the Data Center is independently reviewed by Information Security.	N/A	N/A	N/A

IV. IT Operations - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
IT Operations	High	Servers and other hardware components in the data center and computer rooms may fail to operate as expected because the data center and computer rooms are not appropriately protected from the environmental risks. This may cause unexpected business interruptions and expose the Bank to adverse financial, operational and regulatory risk and issues.	Strong	The Scarsdale and Chanin Data Center are adequately protected by the appropriate environment controls.	N/A	N/A	N/A
Business Application Report	Moderate	Information from business applications reports may be inaccurate or unsecured, because the production environment is not appropriately and adequately protected. This may expose the Bank to adverse financial, operational and regulatory risks and issues.	Strong	Reports are generated directly from the Applications and are distributed to the Business Units with out alterations. For each new release, upon User Acceptance testing the Reports contents are validated to ensure that the output is accurate.	N/A	N/A	N/A

IV. IT Operations - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Monitoring of System Resource and Performance	Moderate	The production system may perform sub-optimally or degrade because it is not appropriately and adequately monitored. This may cause unexpected business interruptions and expose the Bank to adverse financial, operational and regulatory risk and issues.	Strong	System resources and performance of key components of the Bank's IT infrastructure (CPU, server memory, routers, switches, bandwidth, network devices, etc.) are monitored. Issues, including possible malfunctions or disruptions are addressed timely and appropriately.	N/A	N/A	N/A
Performance Metric Reporting	Moderate	The production system may perform sub-optimally or degrade because the system monitoring metrics are not reported to and reviewed at the appropriate level of management. This may cause unexpected business interruptions and expose the Bank to adverse financial, operational and regulatory risk and issues.	Adequate	Key system metrics pertaining to performance, availability and reliability are reported to and reviewed by the CTO.	N/A	N/A	N/A

IV. IT Operations - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
In house Managed Systems (MISER)	High	The overnight process may generate incorrect results because the process is not adequately and appropriately supported by tools and processes. This may expose the Bank to adverse financial, operational and regulatory risk and issues.	Strong	The tool for the overnight process is appropriately configured for optimal performance and security. The overnight environment (jobs, schedule, applications, etc.) is subject to IT Change Management process. An operator monitors the overnight process. Issues are automatically reported so that they can be addressed appropriately and timely in order to minimize disruptions. The report of the overnight job status is generated and reviewed after the completion of the overnight job.	N/A	N/A	N/A

V. Business Continuity Planning (BCP) - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Disaster Recovery	High	The Bank may fail to adequately recover its technology systems following disruptive and unexpected events, due to incomplete Disaster Recovery plan. This may result in broad and negative impact to the Bank.	Weak	The BC/DR Team facilitates the development, testing and readiness of the disaster recovery plans ("DRP") for the Bank's in-house hosted critical applications/systems. The relevant DRP's are activated after the declaration of a disaster, so that the appropriate people, processes and procedures are in place to recover the Bank's technology systems in order to resume the appropriate business operations following unexpected disruptions. The DRP's address both the Cyber related and non-Cyber related events. The BC/DR Team validates the testing and readiness of the disaster recovery plans for critical vendor-hosted applications.	The DRP is no longer included in the BCP-2021. However, a bank-wide DRP has not been published to address the recovery of all critical systems and applications, both in-house and/or vendor-hosted, for interruptions that are caused by cyber-related and non-cyber related disasters	The IT centric Disaster Recovery Plan will be separated from the enterprise business continuity plan. The DRP is planned to be finalized along with the Bank's plan for cloud services on AWS. *(Related to an existing Audit Issue.)*	7/31/2022

V. Business Continuity Planning (BCP) - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
BCP/DR	High	The Bank may fail to timely and adequately respond to disruptive and unexpected events, due to incomplete, inappropriate, outdated or untested Incident Response plan. This may result in broad and negative impact to the Bank.	Weak	The BC/DR Team facilitates the development, testing and readiness of the Incident Response Plan ("IRP") for non-Cyber related incidents. The non-cyber IRP contains the details of the personnel, tools, actions and activities that can be activated, should a non-Cyber adverse event occurs that may result in the loss of information systems and processes. InfoSec facilitates the development, testing and readiness of the Cyber-related incident response plan.	An Incident Response ("IR") Plan should be developed for non-Cyber related incidents.	An Incident Response ("IR") Plan will be developed for non-Cyber related incidents. *(Related to an existing Audit Issue)*	3/31/2022

V. Business Continuity Planning (BCP) - Key Residual Risks - Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Business Continuity Planning	High	The Bank may fail to react quickly and efficiently to disruptive and unexpected events such as natural disasters, cyber attacks or pandemic breakouts, due to inadequate Business Continuity plan. This may result in broad and negative impact to the Bank.	Adequate	The bank wide Business Continuity Plan is consolidated from individual line of business continuity plans ("LOB-BCP"), which are reviewed and approved by the relevant department/division heads at least once a year. Each line of business maintains a separate Business Continuity Plan ("LOB-BCP"). Each LOB-BCP provides the detailed steps and action items to recover and resume the operations for the related line of business in the event of an unexpected disruption. Each LOB-BCP is aligned with and integrated into the bank wide Business Continuity Plan.	The individual LOB BCPs should be submitted to formal review and sign-off by December 2021 and subsequently by the end of the fiscal year on an ongoing basis. BCP-2021 documents the team composition and tasks by business unit, in the event of the loss of major sites (see BCP-DRP for specifics).	Individual LOB BCPs will be submitted to formal review and sign-off.	12/31/21

V. Business Continuity Planning (BCP) - Key Residual Risks - Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Business Impact Analysis	High	The criticality of business activities and associated resource requirements may not be adequately determined without a systematic business impact analysis. This may result in the Bank failing to ensure operational resilience and continuity of operations during and after a business disruption.	Adequate	Business Impact Analysis has been completed by the Bank for each Business Unit which identifies the business functions and prioritizes them in order of criticality and assesses a disruption's impact. The BIA defines the recovery priorities and resource dependencies for critical processes.	N/A	N/A	N/A
Pandemic Planning	High	The Bank may fail to timely and adequately respond to a pandemic, due to incomplete, inappropriate, outdated Pandemic plan. This may result in broad and negative impact to the Bank.	Adequate	A Pandemic Plan is developed, tested and ready to be activated in order to ensure that processes and procedures are in place to respond adequately to a possible outbreak. The Plan is presented to TOPC for approval.	N/A	N/A	N/A

V. Business Continuity Planning (BCP) - Key Residual Risks - Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
BCP/DR	High	The Bank may fail to timely and adequately respond to an unexpected business disruption, due to inadequately and untimely testing of Business Continuity Plan and Disaster Recovery Plan. This may result in broad and negative impact to the Bank.	Adequate	The relevant line of business updates the line-of-business' Business Continuity Plans ("LOB-BCP"), the Business Impact Analyses ("BIA") and the Incident Response Plans ("IRP") to keep the plans relevant in a timely manner. The Business validates the Disaster Recovery Plans ("DRP") and subsequent test results from IT and critical vendors. The updates occur at least once a year, or when there are major changes to the Bank's business, operations or technology. Updates are also performed after the testing of the BCP and DRP, should there be changes resulting from the testing.	There should be a communication to the owners of the BCPs and DRPs about their responsibility in the maintenance of the respective BCPs and DRPs. Appropriate controls should be designed and implemented to ensure that BCP/DRP are updated upon major changes in the Bank (people, process, technology, legal, etc.) or after a test of a BCP and DRP .	Individual LOB BCPs will be maintained when submitted to formal review and sign-off.	12/31/2021

V. Business Continuity Planning (BCP) - Key Residual Risks – Moderate and Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Reporting *(Moderate Residual Risk)*	High	The stakeholders may not be aware of the testing results, due to incomplete, inappropriate, untimely BCP-DRP reporting. This may result in resources insufficiently deployed in the event of a business disruption, which in turn mat cause broad and negative impact to the Bank.	Adequate	A report on the status and test results of the Business Continuity Plan and the Disaster Recovery Plan is regularly provided to the CTO, the Technology and Operations Planning Committee (TOPC) and the Operations and Technology Committee (OTC) of the Board.	N/A	N/A	N/A
Business Interruption Insurance *(Low Residual Risk)*	Moderate	The Bank may not recover losses from unexpected disaster or business disruption because inadequate insurance coverage. As a result, this may result in negative financial impact to the Bank.	Adequate	The BC/DR Team works with Legal to validate the continuance of the appropriate insurance policies to cover key and significant Cyber-related and non-Cyber related risks for unexpected business disruptions at the Bank.	N/A	N/A	N/A

VI. Infrastructure - Key Residual Risks - Very High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Network Access Control	Very High	Devices could be attached to the Banks Network and go undiscovered. This could result in loss of control over the Network and further infiltrate systems and applications.	Weak	The Bank has implemented Network Access Control (NAC) which would provide the Bank the ability to implement stronger security measures.	The Bank has not completed the Network Access Control (NAC) project. Consequently, the rating of this control remained unchanged from that of 2020.	The Bank is implementing the NAC project.	10/31/21 (Completed)
Network Architecture	Very High	Proper Network Segmentation would reduce the Network Attack impacts. Without an effective approach, management may not be able to minimize the impact in the event of a malicious attack.	Weak	The Bank has implemented Network Segmentation which would provide the Bank the ability to implement stronger security measures.	he Bank has not completed the Network Segmentation project. Consequently, the rating of this control remained unchanged from that of 2020.	The Bank is implementing the network segmentation project.	Spreadsheet – 6/30/21 Debi - 11/30/21 Joe – 3/31/22

VI. Infrastructure - Key Residual Risks – High and Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Identity and Access Management (Infrastructure) *(High Residual Risk)*	Very High	Individuals may have excessive or unauthorized access to operating system, database, network or application. This permits individuals or malicious parties with access to the individuals' account to perform functions and execute transactions that may be inconsistent with the individuals job function.	Adequate	User access is authorized and an IAM (Identity Access Management) process is established for all networked and applications. This includes maintaining the proper segregation of duties between approved and implementer of any user change.	N/A	N/A	N/A
Change Control and Configuration Management *(Moderate Residual Risk)*	High	Access may not be appropriately restricted to the firewall which could lead to unauthorized changes. Palo Alto / CISO FTD - FirePower Threat Defense Only the Networking group is authorized to make changes to the firewall configuration. Info Security has only read access to the firewall configuration/rule sets.	Adequate	Access to firewalls is restricted to designated IT professionals. All changes to the firewalls must follow the Bank's Change Management Policy. A reconciliation is performed between the changes in Firewall rules and the Solar Wind Log.	N/A	N/A	N/A

VI. Infrastructure - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Identity and Access Management (Infrastructure)	Low	Access to the privilege accounts of the Bank's infrastructure, if unauthorized or inadequately managed, may expose the Bank to privilege misuse and attacks from both internal and external malicious actors	Strong	Access to privileged Network accounts is limited to appropriate individuals	N/A	N/A	N/A
	High	Users access may not be tied to a single sign on solution, which increases the risk to the Bank via multiple paths of access to the Banks Systems.	Strong	The Bank implements Single-Sign On, which would provide the ability to implement stronger security measures.	N/A	N/A	N/A
Vendor Security	Moderate	The company may not have a complete list of their Service Providers which could allow services to continue without review and permit ongoing vendor access to their systems.	Adequate	Access is only granted to employees of a Service Provider that is listed in ABS Vendor Management's "vendor list."	N/A	N/A	N/A

VI. Infrastructure - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Network Security	Low	Access controls may not be in place to prevent unauthorized individuals from gaining entry into the Bank's Systems as controls may not be in place to authenticate remote access users.	Strong	Remote access communications to the Bank's Corporate Systems are authenticated, encrypted and monitored. Remote access to ABS information assets using bank-issued devices is secured by Virtual Private Network (VPN). Authentication of remote access using bank-issued devices is secured by MFA (multi-factor authentication) in OKTA, which is integrated with ABS Active Directory. Idle access session requires user to re-authenticate Remote access to ABS information assets using non bank-issued devices is secured by Virtual Desktop Infrastructure (VDI). Remote Desktop Protocol ("RDP") to connect to their Computing Devices is restricted	N/A	N/A	N/A

VI. Infrastructure - Key Residual Risks – Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Threat and Vulnerability Management (Infrastructure)	Moderate	IT resources could be compromised and business operations could be disrupted due to a virus without effective updates to servers and workstations.	Strong	All network devices have an endpoint protection solution installed. Daily automatic local scans for potential threats are scheduled. Anti-malware software and definition files are set to automatically receive the latest updates. The ability to disable or remove anti-malware programs is restricted.	N/A	N/A	N/A
	Low	Without an effective patch management identification process IT resources could be compromised and business operations could be disrupted.	Strong	Required security patches are regularly identified and assessed by regularly reviewing and assessing threats and vulnerabilities Security patches are tested before being installed to the production environment . A remediation/validation scan is performed to ensure that the vulnerabilities are eliminated due to the installation of the patch.	N/A	N/A	N/A

VI. Infrastructure - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Information Transfer	High	Access controls may not be in place to prevent unauthorized individuals from gaining entry into the Bank's Email System. Further, malware could be introduced which could lead to a disruption in processing	Strong	E-mails and e-mail systems are protected from unauthorized access, modification or denial of service, spam and phishing emails, malicious e-mails, attachments and the leaking of non-public information. E-mails with non-public information must be authorized. Its information is masked or encrypted.	N/A	N/A	N/A

VII. Data Classification - Key Residual Risks - High

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Data Classification Process	High	Incorrect classification of critical data elements can result in the incorrect protection being applied.	Weak	The Bank has established a Data Classification approach so that the company can identify and take all commercially reasonable steps necessary to confirm that its data assets are protected appropriately.	A completed labeling of unstructured data needs to be performed in accordance with the Data Classification Policy.	A project plan will be completed for the classification of unstructured data.	6/30/22
Data Discovery Program	High	Incorrect classification of critical data elements can result in the incorrect protection being applied and result in unauthorized access and/or disclosure.	Weak	Information assets owned, used, created or maintained by the Bank, must be classified into one of four categories: Confidential, Restricted, Internal or Public	A completed labeling of unstructured data needs to be performed in accordance with the Data Classification Policy.	A project plan will be completed for the classification of unstructured data.	6/30/22

VII. Data Classification - Key Residual Risks - Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Network Controls Processes	High	Transmission of confidential data may result in unauthorized disclosure of confidential bank information	Adequate	Confidential and Restricted Data Control - Unauthorized transmission through any electronic messaging system (e-mail, instant messaging, text messaging) is prohibited.	N/A	N/A	N/A
Encryption Processes	High	Transmission of confidential data in clear text may result in unauthorized disclosure of confidential bank information	Adequate	Authorized transmission for Confidential and Restricted data must use encryption for data in transit and maintained at rest. The encryption must, at minimum, meet the standards specified in the Bank's Encryption Standards.	N/A	N/A	N/A
Access Controls and IAM Program	High	Incorrect Access Controls of critical data elements can result in unauthorized access and/or disclosure.	Adequate	Confidential, Restricted and Internal information is intended primarily for use within the organization and access is limited to those with "business need-to-know" and non-Bank personnel covered by a non-disclosure agreement. Access is limited to employees and non-Bank personnel subject to a non-disclosure agreement.	N/A	N/A	N/A

VII. Data Classification - Key Residual Risks - Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
DLP Monitoring Processes – Confidential Data	High	Unauthorized disclosure of data is increased without the use of various software and data protection programs/processes.	Adequate	Protections against data leaks are implemented for confidential and restricted data.	N/A	N/A	N/A
Monitoring Program	High	The use of incorrect tools may not detect any issues in data protections	Adequate	Information Security uses a variety of tools to monitor and assess whether data security controls and measures have been implemented and are being followed.	N/A	N/A	N/A
Data Protection and Access Controls	High	Unauthorized Disclosure of confidential data including PII is increased without the use of Multifactor Authentication	Adequate	Confidential Data Control - Multi factor authentication is required to access data.	N/A	N/A	N/A

VII. Data Classification - Key Residual Risks - Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Training on Data Classification Policies	Moderate	Employees incorrect application of data classification standards to critical data elements can result in the incorrect protection being applied.	Adequate	Training is provided to employees in regard to Data Classification Requirements.	N/A	N/A	N/A
Removal / Destruction of Expired Data / Devices	Moderate	Data which is not removed on a timely basis is subject to unauthorized disclosure or use.	Adequate	Confidential Data Control - Destruction of data based on data retention policy.	N/A	N/A	N/A

VIII. Encryption - Key Residual Risks - High/Moderate

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Key Management *(High Residual)*	High	Without the proper management of encryption keys - the possibility of the recoverability of encrypted data and unauthorized use of keys to access confidential data is increased.	Weak	There shall be a process to manage the Keys (CA Certificates). This includes creation, distribution, changing, recovery of encryption keys at Apple Bank.	There needs to be a development of a centralized Process and Procedures key management that will accommodate various applications and devices within Apple's environment.	Software for key management is being evaluated and once it has been identified a project plan will be put in place for implementation.	12/31/21
Data Classification Processes – Confidential Data & Security Application Risk Review Process *(Moderate Residual)*	High	Weak Encryption applied to System and application data may result in unauthorized disclosure and access to compromised sensitive information.	Adequate	Apple bank employed encryption strength based upon the classification of the data.	N/A	N/A	N/A
Enterprise Wide Encryption Processes *(Moderate Residual)*	High	System and application data may be compromised, resulting in unauthorized access to sensitive information.	Adequate	Full disk encryption is required for all Bank physical and virtual technology assets (e.g., Bank-issued laptops, workstations, virtual machines ["VM"] and physical & virtual servers.	N/A	N/A	N/A

VIII. Encryption - Key Residual Risks – Low

Key Process	Inherent Risk Rating	Residual Key Risk	Control Rating	Control Summary	Issue/Finding	Action / Recommendation	Due Date
Security Application Risk Review Processes	Moderate	Weak Encryption applied to System and application data may result in unauthorized disclosure and access to compromised sensitive information.	Adequate	Encryption methods should be reviewed periodically to ensure that the types and methods of encryption are still secure as technology and threats evolve. *(This is a non key control and was tested.)*	N/A	N/A	N/A
IT Infrastructure	Moderate	Unauthorized access to encryption keys may result in unauthorized access and disclosure of confidential data	Adequate	Unencrypted keys must not be stored with the data that they encrypt. *(This is a non key control and was tested.)*	N/A	N/A	N/A

Appendix 1

1.1 Change Management

The aggregate inherent risk in 2021 was revised to “high" from “very high" in 2020, because of the following (as per Operational Risk Management’s RCSA Procedures):

Risk 3 "Risk of implementing a change that has not been approved": revised to "high" from "very high“, because we assessed both the regulatory impact and the customer impact as "moderately significant", which is an assessment of the risk and impacts of Risk 2: "Risk of implementing a change that has not been appropriately assessed”.

Risk 7 "Risk of implementing a change that has not been tested": revised to "high" from "very high“, for the same reason as above. In addition, our Change Management Policy recognizes that some pre-deployment testing cannot be performed because the challenges in creating a test environment that replicates that of the production environment.

Risk 11 "Risk of implementing a change that does not have a back-out plan”: revised to "moderate" from "very high“, because we assessed the regulatory impact as *none* and the customer impact as *moderate*.

1.2 Business Continuity Plan (BCP) / Disaster Recovery Plan (DRP)

The aggregate inherent risk in 2021 was revised to “high" from “very high" in 2020, because of the following (as per Operational Risk Management’s RCSA Procedures):

Risk 1 "Risk that the BCP is inadequate": revised to "high" from "very high”, because we assessed both the regulatory impact and the customer impact as "moderately significant".
Risk 2 "Risk that the Business Impact Analysis (BIA) is inadequate": revised to "high" from "very high“, because we assessed both the regulatory impact and the customer impact as "moderately significant".
Risk 4 "Risk related to incomplete DRP“: revised to "high" from "very high“, because we assessed both the regulatory impact and the customer impact as "moderately significant”.
Risk 5 "Risk related to untested Incident Response Plan (IRP)": revised to "high" from "very high”, because we assessed both the regulatory impact and the customer impact as "moderately significant".
Risk 6 "Risk related to the Pandemic plan is inadequate": revised to "high" from "very high”, because we assessed both the regulatory impact and the customer impact as "moderately significant".
Risk 8 "Risk related to inadequate reporting of BCP-DRP status“: revised to "high" from "very high“, because we assessed both the regulatory impact and the customer impact as "moderately significant“.

Notes: The IT RCSA and associated controls testing was performed with the BC/DR team, which is conducting a comprehensive review of the Bank’s BC/DR environment.