

# **IT Strategic Plan and Budget 2022 - 2024**

**CONFIDENTIAL**

# Contents

<b>Area: Core Systems &amp; Logical Access Control</b>	<b>6</b>
Sub-Area: IBS Change Management	6
Build out the IBS Core Change Management Area	6
Sub-Area: FCM	7
Build FIS Content Management (FCM) Department	7
Document and Report Retention	7
Cypress Upgrade	8
Docuware Administrator Training	8
Sub-Area: Systems and Standards	8
Rename the Systems and Standards Area to IBS Core Support	8
Build Out the Systems and Standards (IBS Core Support) Area	9
Train all Systems and Standards (IBS Core Support) on the Features and Functionality of the New Core System	9
Sub-Area: Logical Access Control	10
Build Out and Continue to Structure the User Entitlement Department	10
Continue to Migrate the Access Management of all the Bank's Critical and Newly implemented Systems, Under One Umbrella within the User Entitlement Area.	11
Implement Role Based Access	12
<b>Area: Digital Applications/Channel &amp; Business Services Support</b>	<b>14</b>
Sub-Area: Digital Application Support	14
Q2 Conversion Pre-engagement SOW with IBS	14
Q2 Integration with IBS (Main conversion)	14
Q2 Wire Integration with Finastra	15
FIS/D1 Online Account Opening (OAO) integrated solution with IBS	15
FIS/D1 Online Account Opening (OAO) Q2/ Integration	16
APB Customer to Customer Transfer	16
General P2P – Person to Person transfer	16
Enhanced Bill Pay / FIS Fusion	17
RFP: New Online Banking Product	17
Sub-Area: Digital/EFT Channel Support	18
Visa Integration with IBS (Includes ATM Conversion)	18
ATM Activate Enterprise Upgrade	18
Transition to Managed Card services / Issue NFC/Contactless Card	19
Sub-Area: Loan Technology Support (Remote Lender, McCracken)	19
C&I in Remote Lender	19
Commercial Loans Data in Enterprise Data Warehouse (EDW)	20
Build Secondary / Failover connectivity for McCracken @Scarsdale	20
Remote Lender Upgrade	21
Upgrade McCracken to v20	21

Sub-Area: Business Services	21
Core Conversion Integration: Verafin, Bus RDC, Positive Pay	22
<b>Area: Enterprise Data Management</b>	<b>23</b>
Sub-Area: Enterprise Data Warehouse (EDW)	23
Build an Enterprise Data Warehouse	23
Sub-Area: Business Intelligence	23
Develop Custom Operational Reporting for IBS	24
Develop Reference Resources Supporting Target Data Environment	24
Implement Data User Tools	25
Sub-Area: Data Operations	25
Re-Create Bank Extracts & Interfaces for IBS	25
<b>Area: Financial Crimes Compliance (FCC) Support</b>	<b>27</b>
Sub-Area: FCC - IT Support	27
Establish IT Support Team for FCC IT Processes	27
Implement Internal Suppression Rules Creation	27
Implement ServiceNow for Rules Workflow	28
New Interface to ACH Tracker	28
Data Feeds to Verafin	29
Modify Existing Screening Processes for Core Conversion	29
Automate Existing McCracken Screening Processes for Accuity, RDC and Verafin using EDW	30
Enhance Existing Alert System	30
Automation of SWIFT Messages Screening	31
Automation of Vendor Management Screening	31
Develop an Internal Website for Data Reconciliation and Ad Hoc Screening	32
Optional: Implement Real Time Sanctions Screening of Onboarding Customers	32
<b>Area: Infrastructure &amp; Support</b>	<b>34</b>
Sub-Area: Service Desk	34
End of Life/End of Support for OS	34
CDI MSA Advanced Support	34
Core Conversion Initiative	35
Training and Professional Development	35
Desktop Support Group & Security Operations Specialist	35
Secure Print Initiative - PaperCut	36
Sub-Area: Server Infrastructure	36
Office 365 Including OneDrive	36
Horizon VDI Deployment	37
VxRail – Dev Environment	37
Mobile Device Management (MDM)	38
Quantum On Premise Storage	38

DMZ VxRail Cluster	39
VxRail Cluster Expansion	39
Microsoft Support	40
Idera SQL Database Server Monitoring	40
Sub-Area: Network Infrastructure	40
WI-FI Network	40
IP Address Management (IPAM)	42
Isolated DMZ	43
Network Visualizer	44
Refresh EOL / Upgrade Devices for 10G Capabilities	44
Software Defined Wide Area Network (SD WAN)	45
Sub-Area: Operations Quality Control	47
Change Management	47
ServiceNow - Developer	47
Major Incident Management	48
Asset Management Framework - Controls	48
Continuous Monitoring (Unauthorized Change)	49
Infrastructure Monitoring (Monitoring Solution)	49
<b>Area: IT GRC-CM</b>	<b>51</b>
Sub-Area: GRC & Change Management	51
Business Application Service Catalog Update Enhancement	51
Business Process Map Implementation and Maintenance	52
Sub-Area: IT Control Testing	52
Mapping Regulatory Requirements to Bank Control Framework	52
Extraction and Mapping of Current IT Policies and Procedures to Apple Bank Controls Catalog	53
Identification/Documentation of Controls in the Core FIS IBS System	54
Develop Framework of IT Controls for Cloud-hosted Environments	55
Execution of IT RCSA	55
Development of a Continuous Testing/Monitoring Program	56
Sub-Area: Business Continuity & Disaster Recovery Management	56
Manage/Maintain the Information in the Bank's Business Continuity Management System	57
Vendor Business Continuity/Disaster Recovery Management Review	57
Develop the Non-Cyber-Related Incident Response (IR) Plan	58
Business Continuity/Disaster Recovery Exercise (IT Infrastructure – Server/Network)	59
Business Continuity/Disaster Recovery Exercise (Mainframe/Core System)	60
Business Continuity Incident Notification Exercise	61
Business Continuity Incident Notification System Enhancement	61
Continuous Improvement to the Business Continuity/Disaster Recovery Program	62
Upgrade Business Continuity Management System Software	62

<b>Appendix 1: Technology Management Framework (TMF)</b>	<b>64</b>
<b>Appendix 2: Budget</b>	<b>65</b>
Budget Estimates (2022): New Initiatives, Summary	65
Individual Area Budget Plans	65
Enterprise Data Management - Enterprise Data Warehouse	65
Infrastructure & Support	66
Server Infrastructure	66
Networking	66
Service Desk	66
Quality Control	66
Digital Operations	66
Systems and Standards	67
IT GRC-Change Management; Business Continuity/Disaster Recovery	67
Other - All	67

# Area: Core Systems & Logical Access Control

Responsible Manager: Judy Nagle, FVP, Core Systems & Logical Access Control Manager

## Sub-Area: IBS Change Management

IT Sub-Area Responsible Manager: Judy Nagle and TBD

### 1. Build out the IBS Core Change Management Area

- a. Objective: Develop an area within the IT Core Systems area that will be responsible for Change Management within the IBS System. This area will be responsible for coordination of system changes and testing between the Business Units and the Vendor.
- b. Value: There will be one centralized area that will manage changes that must be done by FIS for the IBS System
- c. Risk of Not Implementing: lack of coordination and oversight of the vendor changes
- d. Technology Management Framework (TMF) Alignment: Risk reduction (1D), Audit and regulatory compliance (1E), System Support (2)
- e. Category: Change Management
- f. Tactical Implementation Plan:
  - i. Determine staffing needs for this area.
  - ii. Develop Job Descriptions
  - iii. Recruit, Hire and or transfer to create the functional area
  - iv. Ensure staff is scheduled and fully trained on all aspects of the IBS Core System
  - v. Develop Change Control processes as it relates to the FIS/IBS universe
  - vi. Ensure that the IBS Change Management process is incorporated in the Overall IT change management strategy.
  - vii. Develop change control procedures that will align with the Bank's change control procedures (presentment to CAB committee etc.)
- g. Target Start Date: 02/01/22
- h. Target Completion Date: 08/08/22
- i. Resources Required:
  - i. Internal: A fair estimate without knowing the FIS/IBS for implementing changes would be a manager and two support staff. This will need to be reassessed once the FIS/IBS processes are fully understood.
  - ii. External: N/A
- j. Cost: Estimated cost would be between 250,000 to 350,000 for staffing, plus benefits.

## Sub-Area: FCM

IT Sub-Area Responsible Manager: Joseph Petti

### 1. Build FIS Content Management (FCM) Department

- a. Objective: To build a department to handle FCM content which will include managing cold reports and building workflows
- b. Value: Will eliminate some of the manual processes of report and document sharing
- c. Risk of Not Implementing: Not using the capabilities of the FCM system and converting manual processes into automated processes
- d. Technology Management Framework (TMF) Alignment: 1B, 1C
- e. Category:
- f. Tactical Implementation Plan: Product Training and Working with Business Units
  - i. Training on all system capabilities
  - ii. Work with business units to develop specific workflows for their area
- g. Target Start Date: The target date has begun. Meetings and some training have been
- h. Target Completion Date: Completion of the initial rollout is scheduled for August 2022 but will continue through the end of 2022
- i. Resources Required: Staffing
  - i. Internal: Repositioning of some IT staff
  - ii. External: Hire additional staff if needed
- j. Cost: Would be determined if additional hiring would be needed.

### 2. Document and Report Retention

- a. Objective: To look at developing record retention to be able to set automatic purging of reports and documents.
- b. Value: Remove aged reports and documents that meet the Bank's record retention policy.
- c. Risk of Not Implementing: Reports and documents would remain on systems which would not adhere to policy.
- d. Technology Management Framework (TMF) Alignment: 1C, 1D, 1E, 2
- e. Category: Document Retention and Disposal
- f. Tactical Implementation Plan:
  - i. Develop RFPs as required
  - ii. Identify vendors
  - iii. Implement
- g. Target Start Date: Q3, 2022
- h. Target Completion Date: Q4, 2022
- i. Resources Required:
  - i. Internal: Staff
  - ii. External: Working with 3rd party vendors to build automatic retentions where possible
- j. Cost: TBD - SOWs may need to be developed

### 3. Cypress Upgrade

- a. Objective: Upgrade Cypress to version 9.1.
- b. Value: Keep application current which will improve performance.
- c. Risk of Not Implementing: Application software may reach end-of-life.
- d. Technology Management Framework (TMF) Alignment: 1B, 1D, 3
- e. Category: Application Upgrades
- f. Tactical Implementation Plan: Follow the SDLC process
- g. Target Start Date: Q1, 2022
- h. Target Completion Date: Q2, 2022
- i. Resources Required:
  - i. Internal: Staff; Virtual server with adequate storage space
  - ii. External: N/A
- j. Cost: \$22,000 plus additional storage

### 4. Docuware Administrator Training

- a. Objective: Schedule administrator training.
- b. Value: The training will provide the administrators the ability to support user departments.
- c. Risk of Not Implementing: Not being able to support user departments.
- d. Technology Management Framework (TMF) Alignment: 2, 4
- e. Category: Training
- f. Tactical Implementation Plan:
- g. Target Start Date: TBD
- h. Target Completion Date: TBD
- i. Resources Required:
  - i. Internal: Staff
  - ii. External: Docuware to provide training
- j. Cost: TBD

## Sub-Area: Systems and Standards

IT Sub-Area Responsible Manager: Jackeline Lugo

### 1. Rename the Systems and Standards Area to IBS Core Support

- a. Objective: To better align the identity of the Systems and Standards Department for the future state as we move to the IBS Core System.
- b. Value: Better identification and clarity of the functionality of the Department
- c. Risk of Not Implementing: Continued confusion of what the role and functionality of the department is.
- d. Technology Management Framework (TMF) Alignment: Day to day support (2)
- e. Category: System Support
- f. Tactical Implementation Plan:
  - i. Discuss with Management the feasibility of changing the name from Systems and Standards to IBS Core Support



- ii. Finalize the name and obtain Management approval
  - iii. Notify Human Resources of the Name change
  - iv. Update current job descriptions with the new Department name
- g. Target Start Date: 01/05/22
- h. Target Completion Date: 02/28/22
- i. Resources Required:
  - i. Internal: N/A
  - ii. External: N/A
- j. Cost: N/A

## 2. Build Out the Systems and Standards (IBS Core Support) Area

- a. Objective: To increase Staffing within the Systems and Standards (IBS Core Support) area and create a shift structure that will provide for a broader range of hourly support for the Bank and Back Offices
- b. Value: A more robust support environment to support the new Core system
- c. Risk of Not Implementing: Assistance to Branches and Departments will be delayed due to lack of staffing and coverage
- d. Technology Management Framework (TMF) Alignment: Day to Day support (2)
- e. Category: System Support
- f. Tactical Implementation Plan:
  - i. Build a plan to create shifts that will cover evenings and weekends and remove the current rotational weekend coverage currently being provided by the Systems and Standards Department
  - ii. Obtain Management approval to recruit and hire approximately 6 additional Support specialists
  - iii. Recruit and hire resources for support as proposed to management
  - iv. Onboard and train the additional resources on standard processes and the new Core IBS System
- g. Target Start Date: 12/01/21
- h. Target Completion Date: 03/31/22
- i. Resources Required:
  - i. Internal: approximately 6 new resources will be required to support this initiative
  - ii. External:
- j. Cost: Estimated cost for hiring six additional resources at the average rate of 50,000 is 300,000 plus benefits.

## 3. Train all Systems and Standards (IBS Core Support) on the Features and Functionality of the New Core System

- a. Objective: Retrain all Systems and Standard (IBS Core Support) staff on the IBS System so they are ready to perform their new duties related to Bank control to ensure they are ready to provide support the Branches and Back Office at go live on 8/8/22
- b. Value: To have a centralized support that is knowledgeable and able to provide the support needed to all Branch and Back Office Personnel

- c. Risk of Not Implementing There will be no centralized area within the Bank that users can turn to for support on the IBS System
- d. Technology Management Framework (TMF) Alignment: Day to day support
- e. Category: System Support
- f. Tactical Implementation Plan:
  - i. Ensure all staff are included in the Training Plan for all components of the IBS System
  - ii. Ensure that staff completes all self-paced training to ensure they acquire the knowledge needed to support the bank and perform the Bank Control functions
  - iii. Create a practice environment where staff can practice what they learn
  - iv. Obtain any printed resources and guides for staff to refer to
  - v. Assess the staffing needs so the Department can support 82 Branches in addition to the BackOffice areas
- g. Target Start Date: 11/15/21
- h. Target Completion Date: 08/08/22
- i. Resources Required:
  - i. Internal: Current staff in addition to 6 additional resources deemed necessary for Support
  - ii. External: N/A
- j. Cost: There are no additional costs involved to ensure all staff is properly trained and well versed on the System. Training is being provided by FIS. Costs for additional resources have been outlined in a separate work stream.

## Sub-Area: Logical Access Control

IT Sub-Area Responsible Manager: Tamooch Caban

### 1. Build Out and Continue to Structure the User Entitlement Department

- a. Objective: To increase Staffing and build the departmental staffing structure, aligning Management roles, increasing staff and developing a shift structure that will provide for a broader range of hourly support for the Bank
- b. Value: To build and enhance the current User Entitlement area and provide the knowledge and resources to support the ongoing effort of creating a strong, cohesive area responsible for all aspects of Logical Access
- c. Risk of Not Implementing: Regulatory Risks due to the lack of resources needed to perform the necessary functions required to manage, monitor and control user access.
- d. Technology Management Framework (TMF) Alignment: Risk (1D), Audit and Regulatory (1E) and Day to day support (2)
- e. Category: Logical Access
- f. Tactical Implementation Plan:
  - i. Develop a shift schedule that will provide support for evenings and weekends

- ii. Assess staffing needs based on current and future application responsibilities encompassing the need to support the Bank in the evenings and on weekends
    - iii. Promote existing Assistant Manager to Manager of the Area
    - iv. Develop higher level support roles that will assist the Department Manager
    - v. Propose new staffing initiatives and shift schedule to Management for approval
    - vi. Develop Job descriptions as needed
    - vii. Recruit and hire qualified candidates
  - g. Target Start Date: 11/22/21
  - h. Target Completion Date: 03/31/22
  - i. Resources Required:
    - i. Internal: we would need to increase staffing by six individuals based on the current volume of entitlement provisioning responsibilities, the coverage of shifts and the future responsibilities. Additionally there is consideration for the hiring of a Technical Coordinator that would coordinate the migration, training and developing the documentation needed for all systems being transitioned to the User Entitlement area. This person would also provide support for department management, handle Audit requests and be responsible for maintaining and updating all process and procedures
    - ii. External: N/A
  - j. Cost: The estimated cost to acquire the resources needed to accomplish this initiative is estimated to be between 400,000 and 450,000 not including Benefits.
2. Continue to Migrate the Access Management of all the Bank's Critical and Newly implemented Systems, Under One Umbrella within the User Entitlement Area.
- a. Objective: To continue to centralize the Bank Control functions within an independent area, which will minimize risk associated with Business units making unauthorized changes to user entitlements and granting access to systems that are not conducive to one's job responsibilities
  - b. Value: System access is controlled, maintained and monitored in an area that is independent of the Bank's Business units
  - c. Risk of Not Implementing: Unauthorized changes made to user access, User Rights not removed in a timely manner upon termination and users having more access than what is needed to do their job
  - d. Technology Management Framework (TMF) Alignment: Risk reduction (1D), Audit, legal and regulatory compliance (1E) remediation, Maintenance and Support, day to day operations (2)
  - e. Category: Logical Access
  - f. Tactical Implementation Plan:

- i. Acquire training and develop process for the administration processes of all IBS Core components
- ii. Continue to migrate the provisioning of rights for the remaining applications deemed critical by the bank to the User Entitlement Area.
- iii. Participate and acquire training on Administration of rights for any new systems being implemented by the Bank
- iv. As a phase II Develop a migration plan for all non-critical applications used by the Bank once all critical applications have been migrated.
- v. Migrate the provisioning of Access rights to the User Entitlement area of all non-critical applications.
- vi. Provide support to users as applications are being migrated.
- g. Target Start Date: Already Started
- h. Target Completion Date: For all Critical Applications to be migrated to the User entitlement area, it is anticipated that this would be completed within the 3rd quarter of 2022. This date has been moved out from the original date due to the core conversion efforts.
- i. Resources Required:
  - i. Internal: Additional resources needed, as outlined in the User Entitlement build out plan. All resources, new and existing will be needed to achieve a timely successful migration.
  - ii. External: As a placeholder, may need to consider additional consultants to assist with the work effort if the project starts to fall behind.
- j. Cost: There would be no additional cost except for staffing costs, which are outlined in a separate work stream, unless it is determined that outside resources will be necessary to help achieve the final goal.

### 3. Implement Role Based Access

- a. Objective: To develop a Role Based Access methodology across all applications within the Bank and implement an Identity Access Management system to assist in automating this process.
- b. Value: To reduce Manual processing and Standardize the provisioning of System rights based on User role
- c. Risk of Not Implementing: More chance for error with user rights not being provisioned properly and a very manual, labor intensive process
- d. Technology Management Framework (TMF) Alignment: Risk reduction (1D), Audit, legal and regulatory compliance remediation (1E), Maintenance and Support, day to day operations (2)
- e. Category: Logical Access
- f. Tactical Implementation Plan:
  - i. Work with User Departments to develop security roles based on the functional job titles within their areas.
  - ii. The Security role will be used to create a Role Based matrix that incorporates the rights across all applications within the defined Security roles

- iii. engage several IAM (Identity Access Management) software Vendors, to determine the right fit for our needs
  - iv. Narrow selection to approximately three Vendors and perform enhanced due diligence and the selection of the final Vendor for the Project.
  - v. Initiate contract negotiation
  - vi. Sign contract and determine target start date.
  - vii. Work with the selected Identity Access Management Vendor to integrate the Bank's applications into the IAM software, defining system parameters, loading security roles, defining the processes and creating desktop procedures.
  - viii. Phase 2 will be a continuation of the project, but the scope of this phase would be the logical access control for all network (share) access, that will also be tied to defined roles.
- g. Target Start Date: This has already begun with the creation of roles for the core conversion
- h. Target Completion Date: Final completion for all steps within the plan is anticipated to be 2nd quarter of 2023
- i. Resources Required:
  - i. Internal: User Entitlement, Information Security and Project Management resources will be needed
  - ii. External: Vendor resources will be relied upon for the installation and implementation, and to train and assist in the security role creation
- j. Cost: There is no cost for internal resources. As a placeholder, since an IAM system has not been selected yet, I am estimating approximately \$250,000, plus approximately \$100,000 for implementation and licensing.

# Area: Digital Applications/Channel & Business Services Support

Responsible Manager: Rajesh Kalyanaraman, FVP, Digital Apps/Channels & Bus Svcs Support Manager

## Sub-Area: Digital Application Support

IT Sub-Area Responsible Manager: Rajesh Kalyanaraman and TBD

### 1. Q2 Conversion Pre-engagement SOW with IBS

- a. Objective: Pre-Engagement for Q2 (core conversion)
- b. Value: Pre-engagement includes Q2-FIS/IBS connectivity, Q2 API Validation/Analysis & Config mapping
- c. Risk of Not Implementing: Will impact the commencement & delivery of the main Q2/Core Engagement
- d. Technology Management Framework (TMF) Alignment: Risk Management
- e. Category: Core Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Q2
  - ii. Engage Q2 & FIS; and proceed as per project plan
- g. Target Start Date: Q3 2021 (mid-Oct start)
- h. Target Completion Date: Q4 2021 (mid-Dec)
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support, EPMO
  - ii. External: Vendors Q2 & FIS
- j. Cost: \$36,500 (recurring annual \$3200)

### 2. Q2 Integration with IBS (Main conversion)

- a. Objective: Integrate Q2 with the new FIS Core solution
- b. Value: Connect to the new core to provide better robust services thru OLB platform
- c. Risk of Not Implementing: Old Core FIS/Miser going away
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Risk Management
- e. Category: Core Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Q2
  - ii. Engage Q2 & FIS; and proceed as per project plan
  - iii. Deploy to Production as per Core conversion project plan; after IT & Business validation
- g. Target Start Date: Late Q4 2021 (mid-Dec 2021)
- h. Target Completion Date: Q3 2022 (Aug 8th 2022)

- i. Resources Required:
    - i. Internal: Digital Banking & Digital Application Support, EPMO
    - ii. External: Vendor Q2, FIS
  - j. Cost: \$208,000 (recurring annual \$12,000)
- 3. Q2 Wire Integration with Finastra
  - a. Objective: Initiating wire transfer from OLB platform
  - b. Value: Essential function for Business customers and Business services (Cash Management customers)
  - c. Risk of Not Implementing: Fill a service gap & being competitive in the marketplace
  - d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement
  - e. Category: Enhancement
  - f. Tactical Implementation Plan:
    - i. SOW with Q2
    - ii. Engage Q2 & Finastra for project plan & Implementation
    - iii. Deploy to Production as per Q2 project plan including IT/Business Validation
  - g. Target Start Date: Q3 start (Sep 2022 after conversion)
  - h. Target Completion Date: Q4 2022
  - i. Resources Required:
    - i. Internal: Digital Banking & Digital Application Support, EPMO
    - ii. External: Vendor Q2
  - j. Cost: \$40,000-\$50,000
- 4. FIS/D1 Online Account Opening (OAO) integrated solution with IBS
  - a. Objective: Enable Real time opening of accounts to the core via customer self-service thru OAO
  - b. Value: Enhanced experience in online account opening / Customer acquisition
  - c. Risk of Not Implementing: Continue in the current manual process of opening an account; semi-automated
  - d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Grow Balance sheet, Digital Maturation
  - e. Category: Enhancement
  - f. Tactical Implementation Plan:
    - i. SOW with FIS
    - ii. Project Plan with FIS
    - iii. Deployment in D1
  - g. Target Start Date: Q1 2022 (Jan start)
  - h. Target Completion Date: Q3 2022 (with Core)
  - i. Resources Required:
    - i. Internal: Digital Banking & Digital Application Support, EPMO
    - ii. External: Vendor FIS
  - j. Cost: TBD

## 5. FIS/D1 Online Account Opening (OAO) Q2/ Integration

- a. Objective: Enable Real time opening of accounts via Online banking channel for existing customers
- b. Value: Enhanced experience in online account opening / Customer acquisition
- c. Risk of Not Implementing: Reduced customer experience
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement
- e. Category: Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Q2
  - ii. Get Approval from NPIC/TOPC
  - iii. Project Plan with Q2
  - iv. Q2 deployment
- g. Target Start Date: unknown – Q3 2022 (after Core)
- h. Target Completion Date: Q2 2023 (Jan/Feb)
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support, EPMO
  - ii. External: Vendor Q2 & FIS
- j. Cost: TBD

## 6. APB Customer to Customer Transfer

- a. Objective: Money movement option between two Apple customers having OLB profile
- b. Value: Providing a choice to Apple Customers and another payment option
- c. Risk of Not Implementing: Customer Retention and being competitiveness
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Digital Maturation
- e. Category: Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Q2
  - ii. Get Approval from NPIC/TOPC
  - iii. Engage Q2 for Implementation
  - iv. Deploy to Production as per Q2 project plan including IT/Business Validation
- g. Target Start Date: Q3 start (Sep2022 after conversion)
- h. Target Completion Date: Q4 2022
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support
  - ii. External: Vendor Q2
- j. Cost: \$5,000-\$10,000

## 7. General P2P – Person to Person transfer

- a. Objective: Money movement option between an Apple person and external person
- b. Value: Providing a choice to Apple Customers and another payment option



- c. Risk of Not Implementing: Customer Retention and being competitiveness in the market
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Digital Maturation
- e. Category: Enhancement
- f. Tactical Implementation Plan:
  - i. Decide either P2P with Q2 Zelle or other Q2 products; or with reseller Zelle
  - ii. SOW with the vendor
  - iii. Get Approval from NPIC;
  - iv. Engage vendor for Implementation
- g. Target Start Date: Q1 2023 start
- h. Target Completion Date: Q2 2023
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support, EPMO
  - ii. External: Vendor
- j. Cost: ~150k (1yr) + \$150k recurring; 1st year expense of \$300,000 in 2023

## 8. Enhanced Bill Pay / FIS Fusion

- a. Objective: To transition to a better version of FIS Bill Pay product
- b. Value: Enhanced Customer Experience; Better Bill Pay platform ; new APIs
- c. Risk of Not Implementing: Market Competitiveness
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Upgrade
- e. Category: Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Q2
  - ii. Get Approval from NPIC/TOPC
  - iii. Engage vendor for Implementation
  - iv. Deploy as per Vendor plan
- g. Target Start Date: Q1 2023 start
- h. Target Completion Date: Q3 2023
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support
  - ii. External: Vendor
- j. Cost: TBD

## 9. RFP: New Online Banking Product

- a. Objective: Q2 contract is coming to an end; Undertake RFP & analysis for (potentially) new platform
- b. Value: Enhanced Customer Experience; Better platform; Best of breed
- c. Risk of Not Implementing: Q2 agreement to auto renew
- d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement, Risk Management, Digital maturation
- e. Category: Enhancement
- f. Tactical Implementation Plan:

- i. RFP for vendors; Decide on vendor
  - ii. New SOW/Agreement with vendor;
  - iii. Implementation
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q3 2022
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support, EPMO
  - ii. External: Vendor
- j. Cost: Cost of the RFP \$500,000 (might be in the retail budget)
  - i. TBD (current run rate APPROX \$2M pa – incur from Q3 2023)

## Sub-Area: Digital/EFT Channel Support

IT Sub-Area Responsible Manager: Robert Sovatsky

### 1. Visa Integration with IBS (Includes ATM Conversion)

- a. Objective: Integrate Visa with the new FIS Core solution
- b. Value: Connect to the new core
- c. Risk of Not Implementing: Old Core FIS/Miser going away
- d. Technology Management Framework (TMF) Alignment: Enable Business Improve, Risk Management
- e. Category: Core Enhancement
- f. Tactical Implementation Plan:
  - i. SOW with Visa
  - ii. Engage Visa & FIS
  - iii. Deploy to Production as per Core conversion project plan
- g. Target Start Date: Late Q4 2021 (Nov 2021)
- h. Target Completion Date: Q3 (Aug 8th 2022)
- i. Resources Required:
  - i. Internal: Digital Banking & Digital Application Support, IT, EPMO
  - ii. External: Vendor Visa & FIS
- j. Cost: \$48,800 (\$19,800 in Q1, and \$29,000 in Q3)

### 2. ATM Activate Enterprise Upgrade

- a. Objective: Upgrade ATM software to AE and enable “Tap and Go”
- b. Value: Customer retention, Strengthen brand by enabling “Tap & Go” at the ATM
- c. Risk of Not Implementing:
  - i. Customer Retention and being competitive;
  - ii. (Current Edge 10 ATM software expiring end of 2022)
- d. Technology Management Framework (TMF) Alignment: Industry Alignment, Risk Management
- e. Category: Upgrade
- f. Tactical Implementation Plan:
  - i. SOW with NCR, Visa

- ii. Engage with NCR & Visa for certification
    - iii. Complete cert in the lab with NCR & Visa; Deploy as per NCR/Retail preference
  - g. Target Start Date: Q1 2022
  - h. Target Completion Date: Q4 2022/Q1 2023
  - i. Resources Required:
    - i. Internal: Retail Branch operations, Info sec, Digital Application Support
    - ii. External: NCR & Visa
  - j. Cost: \$130,000-\$150,000
3. Transition to Managed Card services / Issue NFC/Contactless Card
- a. Objective: Transition to Visa Card services (from Thales) and also issue Contactless card
  - b. Value: Customer retention, Strengthen brand by enabling “Tap & Go” for Apple Card holders
  - c. Risk of Not Implementing:
    - i. Customer Retention and being competitive;
    - ii. Vendor Transition (strategic); Reduce operational risk
  - d. Technology Management Framework (TMF) Alignment: Industry Alignment, Risk Management
  - e. Category: Enhancement
  - f. Tactical Implementation Plan:
    - i. Amendment/SOW with Visa
    - ii. Engage with Visa for transition; Build Project plan
    - iii. Sow with FIS for support; Complete Cert with Visa/FIS
    - iv. Deploy as per plan and start issuing contactless
    - v. Decommission agreement with Thales
  - g. Target Start Date: Q4 2022; Project start after core conversion;
  - h. Target Completion Date: End of 2nd qtr 2023
  - i. Resources Required:
    - i. Internal: Retail Digital Banking Services, Digital Application/ EFT Channel Support
    - ii. External: Visa, FIS/Cardbase & Thales
  - j. Cost: Visa Project cost ~ \$20,000

## Sub-Area: Loan Technology Support (Remote Lender, McCracken)

IT Sub-Area Responsible Manager: Faith Burke

### 1. C&I in Remote Lender

- a. Objective: Enable C&I to originate loans IN Remote Lender Platform
- b. Value: Eliminate manual/ paper based origination; reduce risk operation; increase efficiencies; address audit concern

- c. Risk of Not Implementing:
    - i. Audit issue; regulatory concern
    - ii. Continue with manual process; increase risk
  - d. Technology Management Framework (TMF) Alignment: Risk Management
  - e. Category: Onboarding
  - f. Tactical Implementation Plan:
    - i. Project in Progress; commenced Jan 2021
    - ii. Development & Build in progress; target end of Nov
    - iii. Complete UAT in end of Jan 2022; Deploy in Early Feb 2022
  - g. Target Start Date: Q1 2021 - Project in Progress; commenced Jan 2021
  - h. Target Completion Date: Q2 2022 (End of March 2022)
  - i. Resources Required:
    - i. Internal: C&I ; FCC; Loan admin, Underwriting; Digital Application/Loan Technology support
    - ii. External: SDS
  - j. Cost: \$40,000-\$50,000
2. Commercial Loans Data in Enterprise Data Warehouse (EDW)
- a. Objective: Enable commercial loans feed into data warehouse
  - b. Value: Operational Efficiency
  - c. Risk of Not Implementing: DWH maturation
  - d. Technology Management Framework (TMF) Alignment: Risk Management
  - e. Category: Enhancement
  - f. Tactical Implementation Plan:
    - i. SOW with Mck; Project in Progress;
    - ii. Development & Build in progress;
    - iii. Complete UAT and deploy Q1 2022
  - g. Target Start Date: Q1 2021 - Project in Progress; commenced Oct 2021
  - h. Target Completion Date: Q2 2022
  - i. Resources Required:
    - i. Internal: Loan Servicing ; EDW, IT – Technology support, Digital Appl/Loan Technology support
    - ii. External: McCracken
  - j. Cost: \$12,000
3. Build Secondary / Failover connectivity for McCracken @Scarsdale
- a. Objective: Enable McCracken to failover to the secondary in case of issues with Primary connection and vice versa
  - b. Value: Failover avoiding disruption to Business
  - c. Risk of Not Implementing: Increase risk; (Potential) Business Disruption
  - d. Technology Management Framework (TMF) Alignment: Risk Management
  - e. Category: Network Upgrade
  - f. Tactical Implementation Plan:
    - i. Engage with McCracken; SOW
    - ii. Create Project as per McK/APB
    - iii. Deploy as per plan

- g. Target Start Date: Q1 2022
  - h. Target Completion Date: End of Q1 2022
  - i. Resources Required:
    - i. Internal: IT Infrastructure, Loan servicing, Digital Application/Loan Technology support
    - ii. External: McK
  - j. Cost: \$6,700
4. Remote Lender Upgrade
- a. Objective: Upgrade to version 3.5
  - b. Value: Eliminate Java install and multi Browser capability
  - c. Risk of Not Implementing: Continued InfoSec Risk
  - d. Technology Management Framework (TMF) Alignment: Risk Management
  - e. Category: Upgrade
  - f. Tactical Implementation Plan:
    - i. Sow with SDS
    - ii. Deploy as per project plan
  - g. Target Start Date: Q2 2022
  - h. Target Completion Date: Q3 2022
  - i. Resources Required:
    - i. Internal: C&I ; CRE; Infosec; IT Infrastructure, Digital Application/Loan Technology support
    - ii. External: SDS
  - j. Cost: No Cost
5. Upgrade McCracken to v20
- a. Objective: Enable Platform upgrade to be up to date
  - b. Value: Reduce Operational Risk; increase efficiency
  - c. Risk of Not Implementing:
  - d. Technology Management Framework (TMF) Alignment: Risk Management
  - e. Category: Upgrade
  - f. Tactical Implementation Plan:
    - i. Engage with McCracken; SOW
    - ii. Create Project as per McK/APB
    - iii. Deploy as per plan
  - g. Target Start Date: Q4 2022
  - h. Target Completion Date: Q1 2023
  - i. Resources Required:
    - i. Internal: Loan servicing ; IT-Loan technology Support
    - ii. External: McCracken
  - j. Cost: Usually zero cost but McK to evaluate post conversion regarding cost.

## Sub-Area: Business Services

IT Sub-Area Responsible Manager: Sam Streeter

1. Core Conversion Integration: Verafin, Bus RDC, Positive Pay
  - a. Objective: 3rd Party Interface to Core
  - b. Value: As above
  - c. Risk of Not Implementing: Old Core Miser going away
  - d. Technology Management Framework (TMF) Alignment: Enabling Business Improvement,
  - e. Category:
  - f. Tactical Implementation Plan:
    - i. Project in Progress; commenced Jan 2021
    - ii. Development & Build in progress; target end of Nov
    - iii. Complete UAT in end of Jan 2022; Deploy in Early Feb 2022
  - g. Target Start Date: Q3 2021
  - h. Target Completion Date: Q3 2022 (Aug 8th 2022)
  - i. Resources Required:
    - i. Internal: Digital Application/Business Services support, IT, EPMO, Branch Ops, Deposit Ops
    - ii. External: FIS
  - j. Cost: N/A (part of core cost)

# Area: Enterprise Data Management

Responsible Manager: Brian Roitman, FVP,

## Sub-Area: Enterprise Data Warehouse (EDW)

IT Sub-Area Responsible Manager: Brian Roitman

### 1. Build an Enterprise Data Warehouse

- a. Objective: Aggregate and accumulate operational data for business intelligence purposes, and standardize reference data for consistency purposes, making it all available to qualified users in structures, semantics, and formats which best support decision-making.
- b. Value: Operations efficiency and improvement, opportunity identification, risk management, regulatory fulfillment.
- c. Risk of Not Implementing: Slower decision-making, less optimal decisions, actions based on only partial information, siloed perspective. All of which lead to opportunity costs for profitability.
- d. Technology Management Framework (TMF) Alignment: 1A through 3
- e. Category: Data Management
- f. Tactical Implementation Plan:
  - i. Establish connections to data sources
  - ii. Configure repositories
  - iii. Land the source data
  - iv. Cleanse, reformat, and organize the data (staging)
  - v. Accumulate the operational data at lowest level of grain
  - vi. Restructure subsets of the data dimensionally in Data Warehouse
  - vii. Set and maintain user entitlements
  - viii. Support users with resources and documentation
- g. Target Start Date: Work is in progress
- h. Target Completion Date: 2023
- i. Resources Required:
  - i. Internal: data engineers (2, incl. 1 new role), analytics manager, data modeler, data ops manager; collaboration with IT Infrastructure and Info Sec teams
  - ii. External: ETL developer help (contractor), FIS BIC SME (contractor)
- j. Cost: \$376,900 (contractors, Direct Access, Tools)

## Sub-Area: Business Intelligence

IT Sub-Area Responsible Manager: Brian Roitman

## 1. Develop Custom Operational Reporting for IBS

- a. Objective: Reach core conversion Readiness Review with all “Day 1” custom reports developed and acceptance-tested.
- b. Value: Managers have operational reporting in place at time of core conversion
- c. Risk of Not Implementing: Operational blind-spots, poor decision-making on resource allocation, compliance issues
- d. Technology Management Framework (TMF) Alignment: 1A through 2
- e. Category: Business Intelligence
- f. Tactical Implementation Plan:
  - i. Collect business requirements
  - ii. Plan development and testing around talent, application, and data availability
  - iii. Design team-wide development process, tools, workflows, storage, protocols
  - iv. Develop and acceptance-test the reports with consumers, per schedule
  - v. Deploy reports with automated run schedule
- g. Target Start Date: Work is in progress
- h. Target Completion Date: May 2022
- i. Resources Required:
  - i. Internal: 3 report developers (2 open positions)
  - ii. External: 3-4 developer contractors for 8 months
- j. Cost: \$436,200 (contractors)

## 2. Develop Reference Resources Supporting Target Data Environment

- a. Objective: Establish, or help establish, report catalog, data catalog, and master data.
- b. Value: Data consumers enterprise-wide can locate and learn about data assets, leading to better decisions and actions.
- c. Risk of Not Implementing: Value of new data repositories is incompletely realized. Data professionals’ time, across all functions, is wasted on search and error.
- d. Technology Management Framework (TMF) Alignment: 1C, 1E, 3
- e. Category: Data Management
- f. Tactical Implementation Plan:
  - i. Configure and load content into enterprise data catalog, glossaries, etc.
  - ii. Create report catalog for producer and user reference
  - iii. Design and implement master data management program
- g. Target Start Date: Work is in progress
- h. Target Completion Date: 2023
- i. Resources Required:
  - i. Internal: analytics manager, data modeler, data ops manager, ops analyst
  - ii. External: none
- j. Cost: \$177,500 (data catalog)



### 3. Implement Data User Tools

- a. Objective: Maximize data operations efficiency and reliability. Democratize analytics and visualization.
- b. Value: Faster and more durable data operations, better data-based communication from analytics and visualization.
- c. Risk of Not Implementing: Value of new data repositories is incompletely realized. Data professionals' time, across all functions, yields lower benefit.
- d. Technology Management Framework (TMF) Alignment: 1C, 1E, 3
- e. Category: Data Management
- f. Tactical Implementation Plan:
  - i. Tool evaluation
  - ii. Vendor approval and tool procurement
  - iii. Tool deployment & training
- g. Target Start Date: Work is in progress
- h. Target Completion Date: 2022
- i. Resources Required:
  - i. Internal: data engineer, analytics manager, data modeler, data ops manager
  - ii. External: none
- j. Cost: \$45,000

## Sub-Area: Data Operations

IT Sub-Area Responsible Manager: Brian Roitman

### 1. Re-Create Bank Extracts & Interfaces for IBS

- a. Objective: Develop fully automated data extracts, to specification, for all partners, vendors, and government agencies requiring them. Have all ready for core conversion Readiness Review.
- b. Value: Legal and regulatory compliance, planning and analysis, marketing
- c. Risk of Not Implementing: regulatory and/or legal penalties, operational instability
- d. Technology Management Framework (TMF) Alignment: 1D, 1E, 2
- e. Category: Data Management
- f. Tactical Implementation Plan:
  - i. Collect business requirements
  - ii. Marshall sufficient talent
  - iii. Design team-wide development process, tools, workflows, storage, protocols
  - iv. Develop and acceptance-test the reports with vendors & partners, per schedule
  - v. Deploy extract automations per required schedule
- g. Target Start Date: Work is in progress
- h. Target Completion Date: May 2022

- i. Resources Required:
  - i. Internal: Existing Staff
  - ii. External: 2-3 developer contractors for 6 months; software consulting
- j. Cost: \$390,400

# Area: Financial Crimes Compliance (FCC) Support

Responsible Manager: Ram Gandham, FVP, IT FCC Application Support Lead

## Sub-Area: FCC - IT Support

IT Sub-Area Responsible Manager: TBD

### 1. Establish IT Support Team for FCC IT Processes

- a. Objective: Establish a defined support methodology for various FCC interfaces.
- b. Value: Customer satisfaction, defined SLAs, increased up time and avoids process interruptions.
- c. Risk of Not Implementing: Missing of SLAs, negative customer experience and regulatory risk.
- d. Technology Management Framework (TMF) Alignment: 2 - Maintenance & Support - Day-to-day Operations
- e. Category: Support Enhancement
- f. Tactical Implementation Plan:
  - i. Define escalation procedures, SLAs
  - ii. Establish roles and responsibilities
  - iii. Resolve any production issues based on the established SLAs
- g. Target Start Date: Q1 2022
- h. Target Completion Date: On Going
- i. Resources Required:
  - i. Internal: ¼ resource
  - ii. External: None
- j. Cost: N/A

### 2. Implement Internal Suppression Rules Creation

- a. Objective: Implement a BAU process to create suppression rules on a daily / weekly basis.
- b. Value: Significantly reduces workload on disposition resources and improves process speed for transactions and customer screening.
- c. Risk of Not Implementing: Currently the hit rate for Fed wires is at 70%. Apple Bank is adapted to two sets of eyes disposition to release stopped wires. This is a significant work load for two resources and the hit rate will continuously grow as the sanction lists changes and also data changes in the wires. Dispositioning too many matches is resource intensive, time consuming and can be overlooked by a human eye as hundreds of alerts are there to review.
- d. Technology Management Framework (TMF) Alignment: 3 - Enabling Business Improvement Through Assessments and Upgrades
- e. Category: Process Development
- f. Tactical Implementation Plan:
  - i. Evaluate data either using Python or SQL

- ii. Based on the findings, recommend and implement suppression rules.
- g. Target Start Date: Q1 2022
- h. Target Completion Date: On Going
- i. Resources Required:
  - i. Internal: ½ FTE resource - Additional; FCC resources to review and approve the rules
  - ii. External: N/A
- j. Cost: FTE - AVP

### 3. Implement ServiceNow for Rules Workflow

- a. Objective: Rules workflow configuration in ServiceNow.
- b. Value: Clear audit trail of creation of a rule, review of a rule, approval of a rule and implementation of a rule into production. Avoids regulatory risk and future look backs in case of a wrong rule gets implants into production.
- c. Risk of Not Implementing: Look backs and risk of out of regulatory compliance.
- d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance; 3 - Enabling Business Improvement through Assessments and Upgrades
- e. Category: Process Enhancement
- f. Tactical Implementation Plan:
  - i. Implement Creation, Review, Level 1 approval, level 2 approval and release workflow in ServiceNow
- g. Target Start Date: Q2, 2022
- h. Target Completion Date: Q3, 2022
- i. Resources Required:
  - i. Internal: ½ FTE resource - Additional; existing FCC resource
  - ii. External: N/A
- j. Cost: FTE - AVP

### 4. New Interface to ACH Tracker

- a. Objective: Develop new interface between Accuity and ACH Tracker
- b. Value: Automation of IAT screening with new ACH Tracker.
- c. Risk of Not Implementing: Non-compliance with regulations.
- d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal, and Regulatory Compliance
- e. Category: Process Development
- f. Tactical Implementation Plan:
  - i. Develop process to consume and parse IATs from EPN
  - ii. Develop Soap interface with Accuity to screen IATs
  - iii. Develop web service interface with Accuity for case management
  - iv. Develop interface to communicate with ACH tracker
  - v. Develop process to initiate return IAT transactions in NACHA format
  - vi. Develop communication protocols/channel from process to ACH room
- g. Target Start Date: Q1 2022
- h. Target Completion Date: End of Q2, 2022
- i. Resources Required:

- i. Internal:
  - 1. IT - Dedicated resource
  - 2. ACH tracker
  - 3. FCC
  - 4. ACH room
- ii. External: ACH tracker
- j. Cost: N/A

## 5. Data Feeds to Verafin

- a. Objective: Develop new data feeds to Verafin that includes daily files and historic data files
- b. Value: Enhance enterprise AML program
- c. Risk of Not Implementing: Non-compliance with regulatory compliance.
- d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance
- e. Category: Process Development
- f. Tactical Implementation Plan:
  - i. Develop five new data extracts from McCracken to Verafin
  - ii. Develop one new data extract from CXI to Verafin
  - iii. Develop one new data extract from DMI to Verafin
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q2 2022
- i. Resources Required:
  - i. Internal:
    - 1. IT
    - 2. FCC
  - ii. External:
    - 1. Verafin
    - 2. CXI
- j. Cost: N/A

## 6. Modify Existing Screening Processes for Core Conversion

- a. Objective: Changes to existing screening processes for core conversion
- b. Value: Required to screen customer data on daily basis
- c. Risk of Not Implementing: Regulatory non-compliance
- d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance
- e. Category: Process Enhancement
- f. Tactical Implementation Plan:
  - i. Changes to existing MISER customer extract to core for Sanctions Screening
  - ii. Changes to existing MISER customer extract to core for PEP and Adverse Media Screening
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q2 2022
- i. Resources Required:

- i. Internal:
      - 1. IT
      - 2. FCC
    - ii. External: Accuity
  - j. Cost: N/A
- 7. Automate Existing McCracken Screening Processes for Accuity, RDC and Verafin using EDW
  - a. Objective: Change the source for McCracken extract to EDW and fully automate the extract process.
  - b. Value: Automate the entire Mccracken extract process to Accuity, RDC and Verafin.
  - c. Risk of Not Implementing: Decreased data quality and human error
  - d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance
  - e. Category: Process Enhancement
  - f. Tactical Implementation Plan:
    - i. Change the source from DTNL query to EDW database for Accuity sanctions screening extract
    - ii. Develop new extracts from EDW to produce required extracts for RDC
    - iii. Change the source from DTNL query to EDW for customer, address and account extracts to Verafin
  - g. Target Start Date: Q3, 2022
  - h. Target Completion Date: Q4, 2022
  - i. Resources Required:
    - i. Internal:
      - 1. IT
      - 2. FCC
    - ii. External: Accuity, RDC and Verafin
  - j. Cost: N/A

## 8. Enhance Existing Alert System

- a. Objective: Enhance existing Alert notification system of failed IT processes.
- b. Value: For some processes, users are notifying IT regarding a process failure. Enhancing the notification system helps to improve customer satisfaction and increase up time.
- c. Risk of Not Implementing: Operations risk.
- d. Technology Management Framework (TMF) Alignment: 2 - Maintenance & Support, Day-to-day Operations
- e. Category: Support Enhancement
- f. Tactical Implementation Plan:
  - i. Enhance current alert notification system
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q2 2022
- i. Resources Required:

- i. Internal:
      - 1. IT
      - 2. FCC
    - ii. External: Accuity
  - j. Cost: N/A
- 9. Automation of SWIFT Messages Screening
  - a. Objective: Automate current manual sanctions screening of SWIFT messages.
  - b. Value: Avoids regulatory risk, reduces workloads and strengthens enterprise sanctions screening program.
  - c. Risk of Not Implementing: Manual screening of SWIFT messages leading to human errors
  - d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance
  - e. Category: Process Enhancement
  - f. Tactical Implementation Plan:
    - i. Develop interface to consume and parse SWIFT messages
    - ii. Develop Soap interface with Accuity to screen SWIFT messages
    - iii. Develop web service interface with Accuity for case management
    - iv. Develop communications protocols/channel from process to SWIFT room
  - g. Target Start Date: Q2 2022
  - h. Target Completion Date: Q3 2022
  - i. Resources Required:
    - i. Internal:
      - 1. IT
      - 2. Payments Processing Unit
      - 3. FCC
    - ii. External: None
  - j. Cost: N/A
- 10. Automation of Vendor Management Screening
  - a. Objective: Automate name and transaction screening of upcoming vendor management system.
  - b. Value: Avoids regulatory risk, reduces workloads and strengthens enterprise sanctions screening program.
  - c. Risk of Not Implementing: Regulatory non-compliance
  - d. Technology Management Framework (TMF) Alignment: 1E - Audit, Legal and Regulatory Compliance
  - e. Category: Process Development
  - f. Tactical Implementation Plan:
    - i. Develop interface between Vendor management application and Accuity
  - g. Target Start Date: Q2 2022
  - h. Target Completion Date: Q3 2022
  - i. Resources Required:
    - i. Internal:
      - 1. IT

- 2. Vendor management
  - 3. FCC
  - ii. External: None
  - j. Cost: N/A
- 11. Develop an Internal Website for Data Reconciliation and Ad Hoc Screening
  - a. Objective: Develop an internal website that allows users to do data reconciliation and ad hoc screening. Implement single sign on login to the Web site.
  - b. Value: Currently users are reconciling the data based on multiple auto generated emails throughout the day. Currently Apple Bank creates user profiles in Accuity site in order to provide Ad Hoc screening functionality. An internal web site helps to speed up the process and also avoids regulatory risk.
  - c. Risk of Not Implementing: Reduces efficiency and room for human error that can lead to regulatory risk and also decreased operations efficiency.
  - d. Technology Management Framework (TMF) Alignment: 1C - Ongoing Maintenance of Governance Processes
  - e. Category: Process Development
  - f. Tactical Implementation Plan:
    - i. Develop new website for IAT reconciliation
    - ii. Develop new website for ad hoc screening
    - iii. Integrate with single sign-on
  - g. Target Start Date: Q3 2022
  - h. Target Completion Date: Q1 2023
  - i. Resources Required:
    - i. Internal:
      - 1. IT - Additional ½ resource
      - 2. FCC
      - 3. Access Control
    - ii. External: None
  - j. Cost: FTE - AVP
- 12. Optional: Implement Real Time Sanctions Screening of Onboarding Customers
  - a. Objective: Implement real time sanctions screening for new onboarding customers.
  - b. Value: Enhance customer service and avoid regulatory risks.
  - c. Risk of Not Implementing: Delayed sanctions screening and probably a finding from examiners.
  - d. Technology Management Framework (TMF) Alignment: 1C - Ongoing Enhancement of Governance Processes
  - e. Category: Process Development
  - f. Tactical Implementation Plan:
    - i. New real time interface between Core and Accuity
  - g. Target Start Date: Q1, 2023



- h. Target Completion Date: Q3, 2023
- i. Resources Required:
  - i. Internal:
    - 1. IT - Additional ½ resource
    - 2. FCC
  - ii. External: FIS
- j. Cost: FTE - AVP

# Area: Infrastructure & Support

Responsible Manager: Jose Mendez, FVP, Technology Infrastructure & Support Manager

## Sub-Area: Service Desk

IT Sub-Area Responsible Manager: Maria Siegel

### 1. End of Life/End of Support for OS

- a. Objective: Software Asset Management – EOL Notifications & SaaS connections.
- b. Value: Notifications will allow IT to plan for EOL/EOS.
- c. Risk of Not Implementing: Unsupported software will not have security updates which will increase vulnerabilities.
- d. Technology Management Framework (TMF) Alignment: 1C (Ongoing Enhancement of Processes), 1D (Risk Management), 1E (Audit, Legal and Regulatory Compliance)
- e. Category: Software Asset Management
- f. Tactical Implementation Plan:
  - i. Workflow will be created to create notifications.
  - ii. Report creation
- g. Target Start Date: November 2021
- h. Target Completion Date: March 2022
- i. Resources Required:
  - i. Internal: 2-3 ServiceNow Admins
  - ii. External: CDI
- j. Cost: \$40,000

### 2. CDI MSA Advanced Support

- a. Objective: Increase monthly hours to allow for more work to be done.
- b. Value: Allows for ServiceNow enhancements to mature the platform.
- c. Risk of Not Implementing: Backlog continues to increase and enhancements take longer to implement.
- d. Technology Management Framework (TMF) Alignment: Maintenance & Support of day-to-day Operations
- e. Category: ServiceNow
- f. Tactical Implementation Plan:
  - i. Review and sign a new contract.
- g. Target Start Date: October 2021
- h. Target Completion Date: October 2022
- i. Resources Required:
  - i. Internal: 2-3
  - ii. External: CDI
- j. Cost: \$144,000

### 3. Core Conversion Initiative

- a. Objective: RCC consultants will assist with the setup of PCs at branches.
- b. Value: Service Desk team can continue to support the Bank.
- c. Risk of Not Implementing: Reduced coverage on the Service Desk
- d. Technology Management Framework (TMF) Alignment: Maintenance & Support of day-to-day Operations
- e. Category: Core Conversion Project
- f. Tactical Implementation Plan:
  - i. Consultants will build new PCs for deployment to branches.
  - ii. Consultants will install the newly built PCs in the branches.
- g. Target Start Date: 1/1/2022
- h. Target Completion Date: 6/1/2022
- i. Resources Required:
  - i. Internal: 2-3 SD employees
  - ii. External: 2-3 Consultants
- j. Cost: \$55/hour for each external consultant

### 4. Training and Professional Development

- a. Objective: Customer Service Seminar/Workshop
- b. Value: Provide guidance for managing customer expectations. Explain communication styles and how to tailor service to different types of people.
- c. Risk of Not Implementing: Less than optimal customer service.
- d. Technology Management Framework (TMF) Alignment: Maintenance & Support – day-to-day Operations
- e. Category: Professional development/training
- f. Tactical Implementation Plan:
  - i. The training would be divided into 2 sessions to allow for coverage.
- g. Target Start Date: 1/1/2022
- h. Target Completion Date: 12/31/2022
- i. Resources Required:
  - i. Internal: Existing Staff
  - ii. External: Virtual seminar/workshop - Business Training Works  
<https://www.businesstrainingworks.com/virtual-training/customer-service-courses/>
- j. Cost: Approximately \$3,000

### 5. Desktop Support Group & Security Operations Specialist

- a. Objective: Build a desktop support team to address more complex issues.
- b. Value: Further develop the Service Desk support model. Desktop Support & Security Operations Specialist would be an escalation path for SD Tech Support techs. This will allow us to streamline the ticket flow and properly troubleshoot/resolve issues in an effort to minimize escalation. In addition, it will create a career path for junior techs.
- c. Risk of Not Implementing: Increase in aging tickets, unsatisfied customers, lack of a Knowledge Base.

- d. Technology Management Framework (TMF) Alignment: Maintenance & Support – day-to-day Operations
  - e. Category: Service Desk support
  - f. Tactical Implementation Plan:
    - i. Transition an existing SD Tech to Desktop Support.
  - g. Target Start Date: 1/1/2022
  - h. Target Completion Date:
  - i. Resources Required:
    - i. Internal: 1 employee
    - ii. External: 2 employees (temp – perm)
  - j. Cost: \$55-75/hour
6. Secure Print Initiative - PaperCut
- a. Objective: Print management solution.
  - b. Value: PaperCut is a software application designed to help organizations manage printing to minimize waste, save paper and toner while having a secure printing solution.
  - c. Risk of Not Implementing: Paper & toner waste. No secure print solution.
  - d. Technology Management Framework (TMF) Alignment: 1B (Cost Control, Digital Maturation, Sensible Product Line), 2 (Maintenance & Support of day-to-day Operations)
  - e. Category: Core conversion project.
  - f. Tactical Implementation Plan:
    - i. Server build
    - ii. Vendor will install and configure PaperCut
  - g. Target Start Date: 3/1/22
  - h. Target Completion Date: 9/1/22
  - i. Resources Required:
    - i. Internal: 2-3 employees
    - ii. External: 3 consultants
  - j. Cost: \$5,000 for initial setup, then \$2,000/month

## Sub-Area: Server Infrastructure

IT Sub-Area Responsible Manager: Stephen Apruzzese

### 1. Office 365 Including OneDrive

- a. Objective: Migration of Google Workspace to O365 Initiative
- b. Value:
- c. Risk of Not Implementing: Remaining on Google Workspace
- d. Technology Management Framework (TMF) Alignment: 2, 3
- e. Category: Email and Chat Communication
- f. Tactical Implementation Plan:
  - i. Start implementation of O365 accounts and configuration

- ii. Initiate migration of email through Google Workspace to O35
  - iii. Transition MX records from Google Workspace to O365
- g. Target Start Date: Q1 2022
- h. Target Completion Date: 2023
- i. Resources Required:
  - i. Internal: Server Infrastructure Team
  - ii. External: 3rd Party Management
- j. Cost: \$75,000/month + \$300,000

## 2. Horizon VDI Deployment

- a. Objective: Deploy a full VDI Environment in the Cloud
- b. Value: Replacing all local managed devices with a fully connected network. Ensuring management and patching and continuous connection to the Apple Bank network
- c. Risk of Not Implementing: Continuously catching up on Patch Management and Inventory of devices
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Hardware and Computer Management
- f. Tactical Implementation Plan:
  - i. Configure a fully cloud environment to be managed for Virtual Desktops
  - ii. Including Hardening and security standards for cloud access, similar to AWS and VMWare
  - iii. Migrate current configuration and deploy a hardened environment in the cloud
  - iv. Deploy management and gold standards for desktops in the cloud. Similar to our in house VDI but on a corporate scale
- g. Target Start Date: Q4 2022
- h. Target Completion Date: TBD
- i. Resources Required:
  - i. Internal: Server Infrastructure Team
  - ii. External: 3rd Party Management
- j. Cost: \$55,000/month + \$95,000 SOW

## 3. VxRail – Dev Environment

- a. Objective: Utilize non EOL devices in Scarsdale to house a separate virtual environment for development
- b. Value: To house a separate environment for development and Test, this will free up storage and compute consumption of our production environment for development
- c. Risk of Not Implementing: Storage and computer will continue to be used at a rate of production, which will require expansion
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Server Storage and Compute
- f. Tactical Implementation Plan:
  - i. After the conclusion of AWS and Cloud replication, we will look to repurpose the VxRail cluster in Chanin, and relocate it to Scarsdale

- ii. Licensing and reconfiguration of this environment into VCF through our SDDC will be required
  - iii. VSAN configuration, integration in vSphere and license for connectivity will be required along with configuration.
- g. Target Start Date: Q3 2022
- h. Target Completion Date: TBD
- i. Resources Required:
  - i. Internal: Server Infrastructure Team
  - ii. External: Oversight from 3rd party (Insight) will be required
- j. Cost: \$115,000

#### 4. Mobile Device Management (MDM)

- a. Objective: Readdress the deployment and management of Mobile Devices as requested and driven by Information Security
- b. Value: To manage and full control over bank owned applications on mobile devices
- c. Risk of Not Implementing: Documents and information pertinent to the bank remain available on personal devices
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Mobile Device Management
- f. Tactical Implementation Plan:
  - i. Work with Information Security to develop and select the proper vendor for MDM
  - ii. Assist Information Security in deployment and configuration based on security policies and management they require
  - iii. Transfer ownership and management of the newly deployed MDM software and application to Information Security
- g. Target Start Date: Q4 2022
- h. Target Completion Date: TBD
- i. Resources Required:
  - i. Internal: Server Infrastructure Team & Information Security
  - ii. External: Oversight from 3rd party may be required
- j. Cost: \$145,000

#### 5. Quantum On Premise Storage

- a. Objective: Expand the onsite storage for our internal backups.
- b. Value: To sustain the storage required for the rapid growth of server deployment
- c. Risk of Not Implementing: If we fail to have enough backup storage space on this device, then we will not be able to ensure backup capabilities
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Server Backup
- f. Tactical Implementation Plan:
  - i. Push a quote request through our vendor for the expansion of our system
  - ii. Entertain the options of internal storage expansion or an additional storage bay to be added to the existing system
- g. Target Start Date: Q1 2022

- h. Target Completion Date: Q1 2022
  - i. Resources Required:
    - i. Internal: Server Infrastructure Team & Information Security
    - ii. External: Oversight from 3rd party may be required
  - j. Cost: \$60,000
6. DMZ VxRail Cluster
- a. Objective: Add an additional VxRail cluster to support the new DMZ
  - b. Value: In order to enhance security in our environment, and solidify traffic, a new cluster would need to be deployed to handle DMZ traffic.
  - c. Risk of Not Implementing: The current configuration for DMZ is not ideal for security standards. This will ensure compliance and a higher level of security for the flow of traffic to our DMZ
  - d. Technology Management Framework (TMF) Alignment: 2
  - e. Category: Server Configuration
  - f. Tactical Implementation Plan:
    - i. Deploy a 3 node cluster of VxRail nodes
    - ii. Configure the new DMZ environment to be segregated from the entire infrastructure and only allow traffic that is required for maintenance and DMZ appliances
  - g. Target Start Date: TBD - 2022
  - h. Target Completion Date: TBD
  - i. Resources Required:
    - i. Internal: Server Infrastructure Team & Information Security
    - ii. External: Oversight from 3rd party may be required
  - j. Cost: \$350,000
7. VxRail Cluster Expansion
- a. Objective: Expand our storage and memory on the current VxRail cluster
  - b. Value: In order to support the rapid growth of our environment, we are looking to scale up the storage and memory capacity of our current server cluster.
  - c. Risk of Not Implementing: With the growth of our current environment, it has escalated beyond the proposed growth. We are estimating and anticipating our environment to ensure capacity trends.
  - d. Technology Management Framework (TMF) Alignment: 2
  - e. Category: Server Configuration
  - f. Tactical Implementation Plan:
    - i. Expand storage and add SSD hard drives to the current workload domain
    - ii. Expand memory and add new DIMM's to the current workload domain
  - g. Target Start Date: TBD - 2022
  - h. Target Completion Date: TBD
  - i. Resources Required:
    - i. Internal: Server Infrastructure Team & Information Security
    - ii. External: Oversight from 3rd party may be required
  - j. Cost: \$600,000

## 8. Microsoft Support

- a. Objective: Continue our Support plan with Microsoft.
- b. Value: In order to continue our support plan with Microsoft, we are required to enter a new agreement due to Software Assurance being retired in 2020.
- c. Risk of Not Implementing: Without having proper Microsoft Support, we will be required to outsource our support.
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Server Support
- f. Tactical Implementation Plan:
  - i. Engage a new support plan for all Microsoft products
- g. Target Start Date: Q1, 2022
- h. Target Completion Date: N/A
- i. Resources Required:
  - i. Internal: Server Infrastructure Team & Information Security
  - ii. External: N/A
- j. Cost: \$40,000

## 9. Idera SQL Database Server Monitoring

- a. Objective: To enhance our SQL monitoring – Idera offers an application
- b. Value: With the growth of our SQL environment, we are tasked with monitoring detailed processes and performance. Idera has an application that provides this in depth aspect
- c. Risk of Not Implementing: With the tools we currently have, manual process and additional effort for digging into logs is required
- d. Technology Management Framework (TMF) Alignment: 2
- e. Category: Server Configuration
- f. Tactical Implementation Plan:
  - i. Deploy a new server/utilize cloud SaaS solutions to deploy Idera
  - ii. Add monitoring services to critical bank SQL applications
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q1 2022
- i. Resources Required:
  - i. Internal: Server Infrastructure Team & Information Security
  - ii. External: None/Vendor
- j. Cost: \$30,000

## Sub-Area: Network Infrastructure

IT Sub-Area Responsible Manager: Franklin Cabral

### 1. WI-FI Network

- a. Objective: Wi-Fi technology will be used to provide employees and guests with secure access to the local network and internet to devices that are within Wi-Fi range.



- b. Value: Wi-Fi is wireless LAN. It is one of the important technologies of computer networking, it allows the users to connect to the internet technology without the wires, it allows the router to be cordless also, and the network is connected through an access point for the internet.
- c. Risk of Not Implementing:
  - i. Wireless networks allow devices and users to access information in real-time so that they can roam anywhere they want without being removed from the network. This improves their mobility over the old fashioned traditional networking system. Without WIFI Apple Bank the network will not be able to meet Apple Banks digital transformation initiative.
  - ii. Limitations in Bring Your Own Device: Policies in the workplace are becoming more and more popular, and a wireless network more readily facilitates these policies than a wired network
  - iii. Lack of mobility: With a wireless network, employees can access important files and information from anywhere in the office, so they can bring tablets and laptops into meetings and easily pull up reference documents to discuss. This can bring about a whole new layer to your office's productivity.
  - iv. Organization: Plain and simple, wireless networks are just neater since there are fewer wires to worry about, so your office will look more organized. Plus, maintenance is easier since most of it is software-based, not hardware-based.
- d. Technology Management Framework (TMF) Alignment: 3
- e. Category: Network
- f. Tactical Implementation Plan (for all branches, Chanin and Scarsdale): The following are key steps for successful implementation of the wifi network
  - i. Phase 1 -WIFI simulation using a floor plan
    - 1. A wifi simulation is a RF simulation which allows one to visualize the wifi environment. By using a floor plan as input simulation software is used to map walls, doors, and such on to visualize the wifi signal strength (RSSI) in the different locations. This allows us to estimate the number of wireless access points required to comply with the project's wifi demands. It is important to note that a wifi simulation gives a first indication but should always be followed by a wifi site survey on site.
  - ii. Phase 2- Site survey - before the install
    - 1. During a wifi site survey a RF measurement is performed on site. Besides the wifi signal strength (RSSI) also the background interference (noise) is measured. The ratio of both values is called the signal to noise ratio (SNR) and gives an accurate picture of the wifi quality in the different locations. A site survey will always be performed before and after the install of a wireless network. A survey before the install is often a passive measurement. During

this type of measurement the main goal is to map the RF environment so it can be compared with a wifi simulation. Based on the captured data during the survey the number of and/or the position of the access points can be optimized

iii. Phase 3- Installation and implementation

1. During the installation and implementation of your wireless network the access points are installed at the positions as determined during the wifi site survey. Additionally cabling to the layer 2 switches, testing and certification are required.

g. Target Start Date: January 1, 2022

h. Target Completion Date: June 1, 2023

i. Resources Required:

i. Internal: 2 FTEs

ii. External: Insight, Matrix

j. Cost: \$640,000 + \$150,000 for cabling

## 2. IP Address Management (IPAM)

- a. Objective: Infoblox IP Address Management (IPAM) is a method used to plan, track and manage information associated with a network's Internet Protocol address space.
- b. Value: Using IPAM software, administrators can make sure the repository of assignable IP addresses stays up-to-date. IPAM solutions help simplify and automate the administration of several tasks related to IP space management, including writing DNS records and configuring DHCP settings. Other common functionality includes reservation controlling in DHCP plus other data aggregation and reporting capabilities.
- c. Risk of Not Implementing: IT will continue to use excel sheets to track IPs. This poses a risk to the firm since it requires manual labor and can introduce human error resulting in network service impacting issues.
- d. Technology Management Framework (TMF) Alignment: 3
- e. Category: Network
- f. Tactical Implementation Plan
  - i. These are the tasks required to implement your organization's IPAM design:
    1. Install IPAM Server with the server team and vendors support
    2. Choose an IPAM Provisioning Method
    3. Configure Server Discovery
    4. Discover Servers on the Network
    5. Add a Server to Server Inventory
    6. Create IPAM Provisioning GPOs
    7. Configure DHCP Access Settings
    8. Configure DNS Access Settings
    9. Configure DC and NPS Access Settings
    10. Choose Managed Servers
    11. Verify Managed Server Access

- 12. Retrieve Data from Managed Servers
  - 13. Install RSAT and Install IPAM Client
  - 14. Connect to an IPAM Server
  - 15. Assign Roles
  - g. Target Start Date: January 1, 2022
  - h. Target Completion Date: December 31, 2022
  - i. Resources Required:
    - i. Internal: 2 FTEs (Network and Server)
    - ii. External: Infoblox
  - j. Cost: \$150,000
3. Isolated DMZ
- a. Objective: Deploy a demilitarized zone (DMZ) is a perimeter network that will protect our organization's internal local-area network (LAN) from untrusted traffic.
  - b. Value: The DMZ Network exists to protect the hosts most vulnerable to attack. These hosts usually involve services that extend to users outside of the local area network, the most common examples being email, web servers, and DNS servers. Because of the increased potential for attack, they are placed into the monitored subnetwork to help protect the rest of the network if they become compromised.
    - i. Hosts in the DMZ have tightly controlled access permissions to other services within the internal network, because the data passed through the DMZ is not as secure. On top of that, communications between hosts in the DMZ and the external network are also restricted to help increase the protected border zone. This allows hosts in the protected network to interact with the internal and external network, while the firewall separates and manages all traffic shared between the DMZ and the internal network.
  - c. Risk of Not Implementing: A DMZ is an additional layer of security used to protect our systems in the event they are compromised. Apple bank will not be able to limit the damage an attacker can do without a DMZ. The DMZ requires all traffic from the DMZ to pass through a firewall, therefore effectively limiting the damage an attacker can do. Without the DMZ an attacker will have the ability to pivot into the internal network and attack internal systems.
  - d. Technology Management Framework (TMF) Alignment: 1D, 3
  - e. Category: Network
  - f. Tactical Implementation Plan
    - i. Assign DMZ address space - update IP scheme spreadsheet
    - ii. Create DMZ - Apps zone in the firewall
    - iii. Assign ports in DMZ switch stack - build in redundancy
    - iv. Stand up hosts / Vm environment in the DMZ zone - Collaboration with Server team
    - v. Assign Nats as hosts need inbound access
    - vi. Create rules for access from Outside --> DMZ
    - vii. Create rules for DMZ <-> Trusted network

- viii. Create / Update DNS records
    - ix. Create / Update Visio diagram
    - x. Create / Update Rack elevation for all related equipment
  - g. Target Start Date: January 1, 2022
  - h. Target Completion Date: December 31, 2022
  - i. Resources Required:
    - i. Internal: 2 FTEs (Network and Server)
    - ii. External: Insight
  - j. Cost: \$175,000
4. Network Visualizer
- a. Objective: Implement a Network visualization, graph visualization or link analysis is the process of visually presenting networks of connected entities as links and nodes.
  - b. Value: network visualization tools provide a unified view of network connections, applications, dependency relationships, topology, and ADM information. With these network map visualizations, users can see the physical and logical relationships between routers, switches, servers, interfaces, volumes, and groups to quickly isolate and identify critical health and performance issues. Automation allows your team to spend less time troubleshooting and more time focused on your key business objectives. Centralized network automation can alert your team to issues in real time and provide guided remediation, which speeds up the automation process and eliminates human error.
  - c. Risk of Not Implementing: The network team will continue to operate manually without a centralized view of the network. This will continue to introduce the human error factor and prevent the network team from improving their MTTR.
  - d. Technology Management Framework (TMF) Alignment: 3
  - e. Category: Network
  - f. Tactical Implementation Plan: TBD
  - g. Target Start Date: January 1, 2022
  - h. Target Completion Date: December 31, 2022
  - i. Resources Required:
    - i. Internal: 2 FTEs (Network and Server)
    - ii. External: Thousandeyes or LiveNX or Netbrain
  - j. Cost: \$300,000
5. Refresh EOL / Upgrade Devices for 10G Capabilities
- a. Objective: The Network Department in conjunction with Information Security have found network devices in the Bank that are at the end of vulnerability support or have been published in the maker's End of Life list. Said devices cannot be upgraded to address security vulnerabilities and/or put them into maintenance
  - b. Value: Make the company in compliance with regulators and auditors. Improve the performance of systems and applications connected to the Bank's network. Lower the overall risk in the company by diminishing outages and increasing resiliency, self-healing networks

- c. Risk in not doing: The Bank will be out of compliance, vulnerable to cyber-attacks and ransomware. Poor performance of applications and overall low availability of resources
- d. Technology Management Framework (TMF) Alignment : 3
- e. Category : Network, Hardware Refresh
- f. Tactical Implementation Plan:
  - i. Upgrade network devices, this includes:
    - 1. REPLACE ASA-VPN to branches Chanin and Scarsdale-Four Cisco 2130 w 10 g cap (Scar and Chanin)
    - 2. Scarsdale and Chanin FTD -Four Cisco 2130 for 10g cap (Scar and Chanin)
    - 3. DMZ Switch Upgrade currently 24 ports we need 48 ports w 10g capabilities (Cisco Nexus 93180YC) 4 total (Scar and Chanin)
    - 4. Adding a second Internet switch and Internet circuit CHANIN ASR 1001 and 1002 qty 1 (TBD)
    - 5. External switch upgrade at Scarsdale and Chanin need qty 4 Cisco Nexus 93180YC
  - ii. Plan to complete upgrades (December 2022)
- g. Target Start Date: January 1, 2022
- h. Target Completion Date: December 31, 2022
- i. Resources Required:
  - i. Internal : 2 FTEs (Network and Server)
  - ii. External : Insight
- j. Cost : \$ \$525,280

## 6. Software Defined Wide Area Network (SD WAN)

- a. Objective: Software-defined WAN (SD-WAN) solutions leverage corporate WAN and multi-cloud connectivity to protect application performance at the network edge of branch sites. An SD-WAN uses a centralized control function to securely and intelligently direct traffic across the WAN. This increases application performance and delivers a high quality user experience, resulting in increased business productivity, agility and reduced costs for IT.
- b. Value: Lower WAN OPEX and CAPEX. Greater business agility and responsiveness
  - i. Increased application performance across the WAN. Assure business intent with advanced application visibility and control. Robust edge-to-edge security and micro-segmentation
  - ii. Extensibility to 3rd party products via service chaining, SD-WAN technology is that next-generation toolkit. It provides a centralized portal to control and manage all areas of network performance through the cloud. Engineers will have access to analytics and the ability to see trends and the types of services that are consuming bandwidth. SD-WAN gives administrators the tools to pinpoint exactly where bottlenecks occur and the ability to make adjustments on-the-fly to improve network

performance. Ultimately, SD-WAN provides a level of automation that creates a smarter network.

- c. Risk in not doing: The value proposition for SD-WAN is about making the network smarter and optimizing assets already in place by reducing manual change management burdens and regaining any network monitoring capabilities the enterprise lost after migrating some or all of its infrastructure to the cloud. Apple Bank will continue to pay a premium for the VZ MPLS network.
- d. Technology Management Framework (TMF) Alignment : 1E, 3
- e. Category : Network
- f. Tactical Implementation Plan:
  - i. Business case development: Develop the business-case based on cloud access performance, WAN edge consolidation, branch security and application visibility, and not purely relying on WAN cost savings.
  - ii. SD-WAN Product selection: Engage a Service and solution partner with expertise in multiple SD-WAN technologies. The expertise and knowledge across multiple products will help to curtail the product selection cycle.
  - iii. Distributed Internet and Regional ISPs: With Internet getting distributed to branch offices, the selection of the right ISP and their numbers play a role in the overall cost and management complexities. The selection of the right grade of Internet is also a key consideration in Internet cost, performance and availability.
  - iv. Current infrastructure considerations: plan the information gathering on existing infrastructure including the site wise application traffic requirements and configurations to ensure the future SD-WAN policy-based configurations align and address the site-specific requirements. Understanding the applications in the branch/sites will enable right policy-based configuration for the site. Baselining the current infrastructure performance is also important before beginning the SD-WAN rollout to validate the post deployment benefits and performance. Gather the site-specific information and baseline performance before SD-WAN design and deployment.
  - v. Run Pilot Tests: The aim of a pilot test is to observe and record unforeseen issues, determine if we are using the appropriate network access and better understand how to optimize your policies across a controlled set of locations and applications. From the results, we will determine the appropriate measures to take to improve the network to meet the company objectives.
- g. Target Start Date: November 1, 2022
- h. Target Completion Date: December 31, 2023
- i. Resources Required:
  - i. Internal : 3 FTEs (Network)
  - ii. External : Insight
- j. Cost: \$ 2,500,000 (using Cisco Viptela)

## Sub-Area: Operations Quality Control

IT Sub-Area Responsible Manager: Joseph Armenti

### 1. Change Management

- a. Objective: Our current state of Change Management is now allowing us to further improve. The process needs to mature even further as the environment becomes more complex and additional departments are added to the process.
- b. Value: A mature Change Process leads to more control of the environment, engages teams of the on goings within Apple Bank and provides improved records per audit standards.
- c. Risk of Not Implementing: Current State of Change Activity may continue to cause unwarranted outages. Current Process needs an upgrade as it has outgrown it since inception in Fall of 2020.
- d. Technology Management Framework (TMF) Alignment: 3
- e. Category:
- f. Tactical Implementation Plan:
  - i. Add additional Approval Layers, LOB, UAT
  - ii. Base Approval from CI's with linked applications(Owners)
  - iii. Additional Fields on Change Form
    - 1. Additional Information Required
      - a. Pre-Implementation Testing(question)
      - b. Communication Information
      - c. Actual Start ; Actual End Time
      - d. Group Manager Required to sign off POST Implementation
        - i. Must close change request(requirement)
    - iv. Auto Post Implementation Testing Task assigned to named tester
  - g. Target Start Date: 2nd Quarter 2022 (Pending SNOW license and User configs)
  - h. Target Completion Date: WIP
  - i. Resources Required:
    - i. Addition: Change Resource will be warranted as the Change Process grows within the Bank.
  - j. Cost: Enhancements/ No additional cost outside of the current MSA with CDI. Joseph Armenti can also provide Service Now admin duties. (12k/monthly-MSA)
    - i. A RCC Change resource may be needed as change grows. Potential cost \$50-\$60/HR- RCC

### 2. ServiceNow - Developer

- a. Objective: To focus on ServiceNow objectives.
- b. Value: Full Time Access to alleviate any ServiceNow issues and or enchantments that QC group is currently leading. Shorten Enhancement and troubleshooting efforts.
- c. Risk of Not Implementing: Extended break fix resolution times ; Extended Enhancement response and completion; CMDB accuracy in question ;
- d. Technology Management Framework (TMF) Alignment: 2

- e. Category:
  - f. Tactical Implementation Plan:
    - i. Identify Critical Obstacles in Service Now
    - ii. Prioritize Critical Obstacles
      - 1. CMDB
      - 2. Request System
      - 3. Change Enhancements
      - 4. New user onboarding / group workflow creations
    - iii. Address each issue ; resolution ; documentation
  - g. Target Start Date: 1st Quarter of 2022. Pending Available Resource
  - h. Target Completion Date: WIP
  - i. Resources Required: Contract Resource
  - j. Cost: \$50-\$100/HR - Hourly Rate RCC
3. Major Incident Management
- a. Objective: To install/own the Major Incident Module in ServiceNow.
  - b. Value: Single Pane view for Major Incident Manager; Overview Dashboards; Auto Communications
  - c. Risk of Not Implementing: Unclear Major Incident Process.
  - d. Technology Management Framework (TMF) Alignment: 3
  - e. Category:
  - f. Tactical Implementation Plan:
    - i. Research Major Incident Module
    - ii. Add to current instance of ServiceNow
    - iii. Configure for Apple Bank use; templates, communications.
  - g. Target Start Date: As soon as resource is provided/Approval from Sr. Management to add on to Service Now. Cost involved. TBD: 4th Qtr. 2021-1st Qrt2022
  - h. Target Completion Date: 3rd Quarter 2022
  - i. Resources Required:
    - i. Robert Celona runs the Major Incident Management Module. QC team will handle maintenance, installation, enhancements, and configurations.
  - j. Cost: 10k-40k Installation of Module. (SOW will be sought after)
4. Asset Management Framework - Controls
- a. Objective: Control Accurate Data; Control Enhancement Process around Application (APM), Hardware (HAM) and Software (SAM) management.
  - b. Value: Formalize Ownership; work with owners to centralize processes. Focus on HAM and SAM.
  - c. Risk of Not Implementing: Lost of assets, inaccurate reporting, EOL, inaccurate CMDB
  - d. Technology Management Framework (TMF) Alignment: 4
  - e. Category:
  - f. Tactical Implementation Plan:
    - i. Identify pain points
    - ii. Identify Formal Ownership ( Who owns what)



- iii. Document centralized process
- iv. Work to verify data
- g. Target Start Date: APM has already begun formalizing a process. 2nd quarter of 2022.
- h. Target Completion Date: 4th quarter of 2022
- i. Resources Required: N/A
- j. Cost: No Additional Cost.

## 5. Continuous Monitoring (Unauthorized Change)

- a. Objective: Monitor Infrastructure that includes network devices, servers, Active Directory and cross reference Service Now for any open incidents or change requests.
- b. Value: Ability to monitor infrastructure unauthorized changes; determine cause of outages; Service Now integration
- c. Risk of Not Implementing: Unknown changes stay unknown; risk outages
- d. Technology Management Framework (TMF) Alignment: 1D, 1E, 3
- e. Category:
- f. Tactical Implementation Plan:
  - i. Install Third Party Compliance Tool
  - ii. Configure, Set up Tasks, Rules, Notifications
  - iii. Set up Baseline Monitoring
  - iv. Set up Reporting
  - v. Build a process for reporting unauthorized changes
- g. Target Start Date: Pending Sr Management Decision on current vendor. Tripwire
- h. Target Completion Date: 4th Quarter of 2023.
- i. Resources Required:
  - i. Enhancements to monitoring
- j. Cost: 160k per year; with Tripwire Support (Pending InfoSec solutions added)

## 6. Infrastructure Monitoring (Monitoring Solution)

- a. Objective: Install REAL Infrastructure Monitoring
- b. Value: Proactive response to infrastructure outages in real time; Provide Service Desk or NOC Access to Dashboard/Monitoring to be the first line of response for incidents/issues.
- c. Risk of Not Implementing: With no real solution used by the first line of defense (Service Desk) customers know about outages before IT Operations. This does not support a proactive environment.
- d. Technology Management Framework (TMF) Alignment: 1D, 2
- e. Category:
- f. Tactical Implementation Plan:
  - i. Research Solutions
  - ii. Hire Experienced Admin
  - iii. Deploy into Environment
- g. Target Start Date: 2023
- h. Target Completion Date: TBD
- i. Resources Required: Full Time Monitoring Admin

j. Cost: \$50-\$100/HR Contract

# Area: IT GRC-CM

Responsible Manager: Anthony Scarola, FVP, IT GRC & Change Management Officer

## Sub-Area: GRC & Change Management

IT Sub-Area Responsible Manager: Nisha Manjal

### 1. Business Application Service Catalog Update Enhancement

- a. Objective: The objective is to move the responsibility of directly updating the business application services (ServiceNow, Application Portfolio Management, Business Application Services data) to the line of businesses (LOBs) to decrease time required for updating, improve data accuracy and integrity, and provide for enhanced change monitoring.
- b. Value: To streamline the business application inventory process to ensure compliance and encourage accountability and transparency.
- c. Risk of Not Implementing: The risk of not capturing accurate business application service (software) inventory includes an inability to adequately quantify application risk into the Bank's environment, for example, due to inadequate software license management.
- d. Technology Management Framework (TMF) Alignment: 2 (Maintenance & Day-to-Day Operations) - See Appendix 1
- e. Category: Change Management
- f. Tactical Implementation Plan:
  - i. Further develop project plan, utilizing the System Development Life Cycle (SDLC) policy and procedure as a guide
  - ii. Acquire adequate licensing (e.g., ServiceNow site or individual licenses)
  - iii. Work with vendor (CDI) to implement enhanced workflow and automate update notifications
  - iv. Provide notice to department heads regarding new process and LOB responsibilities
  - v. Meet with every department head /application owners (currently ~24 depts.) and identify stakeholders
  - vi. Provide the list of identified stakeholders to Service Delivery team for granting SN APM access
  - vii. Develop and provide a user guide to the LOB; meet with the stakeholders and walk them through the SN system (i.e., provide end-user training)
  - viii. LOBs update when new applications are added, old applications removed
  - ix. Annually, IT GRC-CM team to re-certify all software with LOB
- g. Target Start Date: Q1 2022
- h. Target Completion Date: Q4 2022
- i. Resources Required:
  - i. Internal: LOBs Department Heads Or their Delegates / IT team

- ii. External: CDI (Vendor support)
  - j. Cost: ~25,000 for CDI support
2. Business Process Map Implementation and Maintenance
- a. Objective: To manage the Business Process Maps hosted in the Bank's instance of IBM Blueworks Live. This is the visualization tool which contains the existing business process maps to be migrated from FIS.
  - b. Value: To provide a centralized and streamline process of managing the tool and related access control ensures compliance with Bank policy and procedures.
  - c. Risk of Not Implementing: Risk includes non-compliance with Bank policy and procedures, delays in access to the underlying information, and overall inefficiencies in the management of the process.
  - d. Technology Management Framework (TMF) Alignment: 2 – Maintenance & Support; Day-to-day Operations
  - e. Category: Change Management
  - f. Tactical Implementation Plan:
    - i. FIS is working to update our business process maps within their instance of Blueworks and will be working to export and import the maps into our own Blueworks instance. This should occur before the end of 2021.
    - ii. Once that work is complete and we have all of the process maps, the IT GRC team will be responsible for managing the system (not the maps), to ensure proper change management and user access control is implemented.
  - g. Target Start Date: Ongoing – Started Q3, 2021
  - h. Target Completion Date: Q4, 2022
  - i. Resources Required:
    - i. Internal: EPMO and IT GRC-CM Team
    - ii. External: FIS, Converge/Essextec (reseller; vendor support as needed)
  - j. Cost: N/A

## Sub-Area: IT Control Testing

IT Sub-Area Responsible Manager: Allen Lum

1. Mapping Regulatory Requirements to Bank Control Framework
- a. Objective: Work to ensure that the Bank's IT policies are in compliance with the ever-changing regulatory landscape and that IT Operations are aware of the latest control practices and requirements.
  - b. Value: Ensure a high level of regulatory compliance to mitigate the risk of insufficient controls and future regulatory findings.
  - c. Risk of Not Implementing: Failing a review/audit/attestation and possible exposure and/or weakness in a new technology or system that the Bank has implemented.
  - d. Technology Management Framework (TMF) Alignment: 1E, 1D, 4

- e. Category: Logical Access, System Support, Cloud Computing
- f. Tactical Implementation Plan:
  - i. Identify Key Regulatory Control Requirements such as FFIEC, NYDFS, SWIFT Attestation, etc.
  - ii. Extract and/or inventory controls into a database/library (e.g., MetricStream)
  - iii. Identify which controls are critical and applicable to the Bank
  - iv. Match the controls in item iii. to the Bank's current control framework
  - v. Perform a gap analysis against IT policies
  - vi. Evaluate the results and develop a remediation/action plan
  - vii. Implement a process to update the controls framework when new pronouncements and regulations are announced
- g. Target Start Date: 03/01/2022
- h. Target Completion Date: 06/30/2022
- i. Resources Required:
  - i. Internal: .3 FTE for year 1 - .1 FTE for year 2 and 3
  - ii. External: N/A
- j. Cost: N/A

## 2. Extraction and Mapping of Current IT Policies and Procedures to Apple Bank Controls Catalog

- a. Objective: To extract stated controls from the current IT policies and procedures and Map to the Bank's current controls in MetricStream. In addition these identified controls would be mapped to the current RCSA if not already.
- b. Value: To keep the GRC tool's IT control library in-sync with Bank IT policies and procedures (i.e., help to ensure a high level of integrity) which in-turn provides an accurate control source for various assessments (e.g., RCSA) and issues (e.g., self-identified issues).
- c. Risk of Not Implementing: Confusion and delays related to the "source of truth" between the IT policies and the centralized control catalog (MetricStream).
- d. Technology Management Framework (TMF) Alignment: 1E, 3
- e. Category: Change Management, Logical Access, System Support, Cloud Computing
- f. Tactical Implementation Plan:
  - i. Inventory and/or extracted controls which are stated within Apple Bank's IT Policies and standards.
  - ii. Place the extracted and/or Inventory Control Requirements into a spreadsheet.
  - iii. Match the controls in item ii. to the Bank's MetricStream control catalog.
  - iv. Perform a gap analysis.
  - v. Review analysis with policy owners or MetricStream administrator(s) to ensure accuracy.
  - vi. Map final controls to IT RCSA and obtain concurrence with IT control owners.

- vii. Resolve discrepancies (i.e., add/remove controls from policy, add/remove controls from MetricStream).
  - g. Target Start Date: 01/01/2022
  - h. Target Completion Date: 03/01/2022
  - i. Resources Required:
    - i. Internal: .1 FTE for each of the three years
    - ii. External: None
  - j. Cost: N/A
3. Identification/Documentation of Controls in the Core FIS IBS System
- a. Objective: Work to ensure that the proper IT controls are included in the new core FIS IBS system.
  - b. Value: Reduce expense by applying appropriate/necessary IT controls prior to go-live.
  - c. Risk of Not Implementing: Not implementing a control which may allow unauthorized access and or execution of a fraudulent transaction. Failing a major review/audit/attestation and possible exposure and/or weakness in a new technology landscape that the Bank has implemented. In addition, expenses might be higher due to adding necessary IT controls post-implementation.
  - d. Technology Management Framework (TMF) Alignment: 1E, 1D, 2, 3
  - e. Category: Logical Access, System Support
  - f. Tactical Implementation Plan:
    - i. Identify key regulatory control requirements (FFIEC, NYSDf, SWIFT Attestation, PCI, etc.) and which are critical and applicable to the Bank's environment.
      - 1. Note, we will exclude the review of Identity and Access Controls as these are reviewed by the Information Security group.
    - ii. Gain and record an understanding of the core FIS IBS system on an IT application and infrastructure level to include cloud-based controls as required.
    - iii. Analyze the processes and determine the key control points.
    - iv. Document the controls which may be in the core FIS IBS system. The controls will be risk-assessed by Information Security as part of their risk assessment.
    - v. Determine if new controls must be implemented based on the process analysis.
    - vi. Match the controls in item iv. to the Bank's current control framework.
    - vii. Perform a gap analysis.
    - viii. Evaluate the results and develop an action plan for remediation.
    - ix. Perform a controls review to determine if the identified controls are actually working.
    - x. Evaluate review and develop remediation plans as required.
  - g. Target Start Date: 04/01/2022
  - h. Target Completion Date: 12/01/2024
  - i. Resources Required:

- i. Internal: .3 FTE for each of the two years
    - ii. External: None
  - j. Cost: N/A
4. Develop Framework of IT Controls for Cloud-hosted Environments
- a. Objective: Develop a framework for IT cloud controls to ensure proper cloud-based controls are included in the Bank's policies and procedures.
  - b. Value: Provide a high level of assurance that the Bank's data is protected in the cloud environment from threats toward confidentiality, integrity and availability.
  - c. Risk of Not Implementing: Exposure of the Bank's data to unauthorized parties.
  - d. Technology Management Framework (TMF) Alignment: 1E, 1D, 3, 4
  - e. Category: Change Management, Logical Access, System Support, Cloud Computing
  - f. Tactical Implementation Plan:
    - i. Build a plan for developing a tactical IT control framework in alignment with the Bank's policies and procedures.
    - ii. Obtain industry standard cloud control framework.
    - iii. Obtain a detailed understanding of the Bank's use of cloud services such as AWS IaaS and VMware Cloud Disaster Recovery (VCDR).
    - iv. Perform an analysis of the various control features available in the cloud that the Bank uses or plans to use.
    - v. Identify cloud controls which are applicable to the Bank and determine if they have been implemented.
    - vi. Test the identified cloud controls as part of the IT RCSA process.
    - vii. Evaluate the results and develop remediation/action plans as needed.
  - g. Target Start Date: 03/01/2022
  - h. Target Completion Date: 12/01/2022
  - i. Resources Required:
    - i. Internal: .2 FTE for one year
    - ii. External: none
  - j. Cost: N/A
5. Execution of IT RCSA
- a. Objective: To help ensure that the proper IT controls are in-place and operating effectively.
  - b. Value: Help minimize issues (regulatory, audit, InfoSec, etc.) and findings.
  - c. Risk of Not Implementing: Control failures impacting IT Operations and delivery of services to Bank employees and clients. Increased findings leading to regulatory scrutiny.
  - d. Technology Management Framework (TMF) Alignment: 1E, 1D, 3, 4
  - e. Category: Change Management, Logical Access, System Support, Cloud Computing
  - f. Tactical Implementation Plan:
    - i. Develop the annual RCSA plan/schedule.
    - ii. Update current control matrixes to ensure alignment with policies and underlying IT controls.

- iii. Work with Operational Risk Management (ORM) to determine timing and scope.
- iv. Execute RCSAs.
- v. Evaluate the results and develop a remediation/action plan.
- vi. Develop a final annual report.
- vii. Perform a post RCSA review to determine process efficiencies.
- g. Target Start Date: 1/01/2022
- h. Target Completion Date: 12/31/2022
- i. Resources Required:
  - i. Internal: 1.5 FTE for each year one, 2.0 FTE for year two to three
  - ii. External: None
- j. Cost: N/A

## 6. Development of a Continuous Testing/Monitoring Program

- a. Objective: Develop and implement a program for continuous testing/monitoring of key IT controls.
- b. Value: To help ensure a continuous effective IT control environment.
- c. Risk of Not Implementing: Control failures which impact IT Operations and delivery of services may not be identified for more than a year or since the last RCSA review.
- d. Technology Management Framework (TMF) Alignment: 1E, 1D, 2, 3
- e. Category: Change Management, Logical Access, System Support, Cloud Computing
- f. Tactical Implementation Plan:
  - i. Review current RCSA and identify key controls that would benefit from a continuous testing / monitoring process.
  - ii. Obtain concurrence with the CTO and ORM/IT Risk.
  - iii. Discuss with IT subject matter experts the potential enhancements to the control testing and evidence process as related to continuous monitoring.
  - iv. Design and execute a pilot program with a limited number of key controls.
  - v. Evaluate the results and develop a plan to expand the program to include other key IT controls.
  - vi. Evaluate the process and adjust as needed.
- g. Target Start Date: 1/01/2022
- h. Target Completion Date: 12/01/2024
- i. Resources Required:
  - i. Internal: .3 FTE for each year
  - ii. External: None
- j. Cost: Software – To be included in the IT Infrastructure budget

## Sub-Area: Business Continuity & Disaster Recovery Management

IT Sub-Area Responsible Manager: David James



## 1. Manage/Maintain the Information in the Bank's Business Continuity Management System

- a. Objective: Manage the current Business Continuity/Disaster Recovery Management System to allow for the:
  - i. incorporation of new/updated information gathered during the BIA process, implementation of products/services, the implementation of new systems/applications, and/or staffing changes;
  - ii. management/monitoring of the organization's business continuity plans; and,
  - iii. coordination of the updating/creation of the organization's disaster recovery plans.
- b. Value: BC/DR Program will have up-to-date information that will be used in the event of a business interruption (e.g., loss of data center, loss of building, loss of staff).
- c. Risk of Not Implementing: The program information/data would not be current, and recovery plans could be impacted. Internal/External Audits could result in lower ratings for the organization.
- d. Technology Management Framework (TMF) Alignment: Non-Project Initiatives - 1C, 1D, 1E
- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan:
  - i. Managing BC/DR Information within the BC Management System
  - ii. Review information with business units within the organization
  - iii. Monitoring system/application changes within the organization
  - iv. Coordinate uploads of employee information with HR
  - v. Manage/Monitor the Business Continuity Plans
    - 1. Work the business area to update/complete their BC Plans
    - 2. Work with business area managers to review and approve plans
  - vi. Coordinate the development of Disaster Recovery Plans
  - vii. Work with IT Infrastructure Management to review and update the organization's disaster recovery plans and playbooks
- g. Target Start Date: 01/01/2022
- h. Target Completion Date: 12/31/2022
- i. Resources Required:
  - i. Internal: 2 (Existing)
  - ii. External: 0
- j. Cost: Vendor: Agility Recovery Planner (Current Software) \$15,000

## 2. Vendor Business Continuity/Disaster Recovery Management Review

- a. Objective: Establish a program within the Vendor Management process to be used to evaluate the Business Continuity/ Disaster Recovery program critical (Tier1-Tier2) vendors and Third Party Service Providers.

- b. Value: Ensuring that critical vendors have business continuity/disaster recovery plans in place that support the necessary recovery of services/resources provided to the Bank.
- c. Risk of Not Implementing: May result in the contracting of vendors or third party services providers that do not meet the necessary Service Level Agreements relating to the recovery of the resources or services used by the Bank to perform their critical business processes.
- d. Technology Management Framework (TMF) Alignment: Non-Project Initiatives - 1E, 1C
- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan:
  - i. Develop Business Continuity/Disaster Recovery (BC/DR) Management questionnaire to be used during the Vendor Management review process.
  - ii. Develop BC/DR Management review process.
  - iii. Incorporate BC/DR Management review process, into the Vendor Management Review Program.
- g. Target Start Date: In progress
- h. Target Completion Date: 12/31/2022 (BAU)
- i. Resources Required:
  - i. Internal: 2 (Existing)
  - ii. External: 0
- j. Cost: N/A - Vendor Management is acquiring a new application to be used to manage the Vendor Management Program.

### 3. Develop the Non-Cyber-Related Incident Response (IR) Plan

- a. Objective: The response plan should cover the following topics:
  - i. Listing of non-Cyber related incidents that may cause unexpected business disruptions;
  - ii. Definition of major phases: preparation, detection & analysis; containment, eradication & recovery; and post-event activity;
  - iii. Communication requirements (personnel, vendors, authorities, etc.);
  - iv. Communication protocol standard for each step (e.g. first response), for major disruption scenario (adverse weather, IT outage, etc.);
  - v. Resources (incident responders and tools), roles and responsibilities;
  - vi. Testing of the Plan; and,
  - vii. Review, approval and maintenance of the IR Plan.
- b. Value: The Non-Cyber-Related (NCR) Incident Response Plan will provide guidance to management regarding what is to be done when responding to a related incident, and who is responsible for performing the tasks. Address outstanding RCSA gap.
- c. Risk of Not Implementing: Possible confusion during an event due lack of guidance leading to inappropriate response and delays. Inability to service employees or customers in a timely manner.
- d. Technology Management Framework (TMF) Alignment: Non Project Initiatives and Processes 1C, 1D, 1E

- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan:
  - i. Develop a list of NCR Incidents that would require a corporate response.
  - ii. Develop a process to respond to the identified incidents.
  - iii. Obtain management approval of the incident response plan.
  - iv. Perform tabletop testing on a scheduled basis.
- g. Target Start Date: 12/01/2021
- h. Target Completion Date: 03/31/2022 with testing to follow
- i. Resources Required:
  - i. Internal: 2 (Existing)
  - ii. External: 0
- j. Cost: The current incident notification system is part of the Agility Recovery Planner BCM Software. There is no additional cost to the organization when this module is used.

#### 4. Business Continuity/Disaster Recovery Exercise (IT Infrastructure – Server/Network)

- a. Objective: Conduct network/server disaster recovery exercises to validate the company's ability to:
  - i. recover critical servers and infrastructure equipment within the predefined time frame, and predefined level of data;
  - ii. provide user access to the recovered environment; and,
  - iii. perform critical processing within the recovered environment.
- b. Value: Validation that the organization has the ability to recover from a business interruption; e.g., loss of the data center. Address outstanding Audit issue (19-89 #2A).
- c. Risk of Not Implementing: The risk of not conducting and exercise include:
  - i. non-compliance with internal policies;
  - ii. non-compliance with external policies; e.g., FFIEC, State Regulators; and,
  - iii. no verification that the BC/DR Plans meet the organization's recovery needs.
- d. Technology Management Framework (TMF) Alignment: Non Project Initiatives and Processes 1C, 1D, 1E
- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan: Each exercise project will be managed by the BC/DR Team with coordination from the IT Infrastructure Teams (network and server), and the various business areas. Each exercise will include the following:
  - i. Exercise Scope includes:
    - 1. Exercise Overview
    - 2. Business Benefits
    - 3. Business Objective
    - 4. Business area/unit participants including IT
    - 5. Testing Window (date/time/location(s))
  - ii. Management Approval of Exercise Scope
  - iii. Identify exercise participants

- iv. Train business area participants regarding completion of exercise documentation
- v. Conduct BC/DR Exercise (includes system failover, and business user validation, identify any issues)
- vi. Prepare exercise reports
- g. Target Start Date: Q1/2022
- h. Target Completion Date: Q2/2023
- i. Resources Required:
  - i. Internal: 2 (Existing Staff)
  - ii. External: 0
- j. Cost: ~\$20,000 per exercise – Based on hourly rate of ~\$1,500. Cost will vary based on the exercise scope, number of applications being recovered, bandwidth needed, and storage needed.

## 5. Business Continuity/Disaster Recovery Exercise (Mainframe/Core System)

- a. Objective: Participate in the FIS DR Brown Deer, WI Data Center Exercise of their Core Systems to the FIS Chandler, AZ Data Center to validate the company's ability to:
  - i. access to the recovered environment; and,
  - ii. perform critical business processes within the recovered environment.
- b. Value: Validation that the organization has the ability to access the FIS recovered environment and perform critical business processes
- c. Risk of Not Implementing: The risk of not conducting and exercise include:
  - i. non-compliance with internal policies;
  - ii. non-compliance with external policies; e.g., FFIEC, State Regulators; and,
  - iii. no verification that the BC/DR Plans meet the organization's recovery needs.
- d. Technology Management Framework (TMF) Alignment: Non Project Initiatives and Processes 1C, 1D, 1E
- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan: The exercise will be project managed by the BC/DR Team with coordination from the FIS Network Team, Apple Bank IT Infrastructure Teams (network), and the various business areas. The exercise will include the following:
  - i. Exercise Scope includes:
    - 1. Exercise Overview
    - 2. Business Objective
    - 3. Business area/unit participants including IT
    - 4. Testing Window (date/time/location(s))
  - ii. Management Approval of Exercise Scope
  - iii. Identify exercise participants
  - iv. Train business area participants regarding completion of exercise documentation

- v. Conduct BC/DR Exercise (includes system failover, and business user validation, identify any issues)
  - vi. Prepare exercise reports
- g. Target Start Date: Q4/2022
- h. Target Completion Date: Q2/2023
- i. Resources Required:
  - i. Internal: 2 (Existing Staff)
  - ii. External: 0
- j. Cost: N/A

## 6. Business Continuity Incident Notification Exercise

- a. Objective: Conduct incident notification exercises to validate the company's ability to:
  - i. Send notification to business teams, individuals, and company-wide;
  - ii. Verify contact information of individual staff members; and,
  - iii. Perform critical processing within the recovered environment.
- b. Value: Validation that the organization has the ability to recover from a business interruption; e.g., loss of the data center.
- c. Risk of Not Implementing: The risk of not conducting and exercise include:
  - i. non-compliance with internal policies;
  - ii. non-compliance with external policies; e.g., FFIEC, State Regulators; and,
  - iii. no verification that the BC/DR Plans meet the organization's recovery needs.
- d. Technology Management Framework (TMF) Alignment: Non Project Initiatives and Processes 1C, 1D, 1E
- e. Category: Disaster Recovery Planning and Testing Enhancements
- f. Tactical Implementation Plan:
  - i. Identify exercise participants
  - ii. Validate contact information
  - iii. Conduct Notification Exercise (includes system failover, and business user validation, identify any issues)
  - iv. Prepare exercise reports
- g. Target Start Date: Q1/2022
- h. Target Completion Date: Q4/2022
- i. Resources Required:
  - i. Internal: 2 (Existing Staff)
  - ii. External: 0
- j. Cost: N/A

## 7. Business Continuity Incident Notification System Enhancement

- a. Objective: Replace current incident notification system.
- b. Value: Prompt notification of disasters and instructions for employees to ensure prompt recoverability.
- c. Risk of Not Implementing: Failure to adequately notify employees in the case of a disaster.
- d. Technology Management Framework (TMF) Alignment: 3

- e. Category: Incident Notification Enhancements
  - f. Tactical Implementation Plan:
    - i. Evaluate solutions
    - ii. Select solution
    - iii. Implement solution
  - g. Target Start Date:
  - h. Target Completion Date:
  - i. Resources Required:
    - i. Internal: 2 (Existing Staff)
    - ii. External: 0
  - j. Cost: TBD
8. Continuous Improvement to the Business Continuity/Disaster Recovery Program
- a. Objective: Continually review the current program with the goal of making improvements based on risk appetite, BC/DR Exercises, Incident Management, and Internal and External stakeholder feedback.
  - b. Value: Improvement of the organization's program, ensuring that it is in-sync with the company's goals and objectives.
  - c. Risk of Not Implementing: BC/DR policies and plans become out-of-sync with what the organization needs.
  - d. Technology Management Framework (TMF) Alignment: Non Project Initiatives and Processes 1C, 1E
  - e. Category: Disaster Recovery Planning and Testing Enhancements
  - f. Tactical Implementation Plan:
    - i. Continuous evaluation of policy and procedures with the goal of strong observation of standards set out by NYSDF, FFIEC, and Disaster Recovery Institute International.
    - ii. Continuous review and updating of the organization BC/DR Awareness Training to include modifications to the program.
  - g. Target Start Date: Q1/2022
  - h. Target Completion Date: Q4/2022 (BAU)
  - i. Resources Required:
    - i. Internal: 2 (Existing Staff)
    - ii. External: 0
  - j. Cost: N/A
9. Upgrade Business Continuity Management System Software
- a. Objective: Evaluate other Business Continuity Management Systems to replace the existing system (RPx) used by Apple Bank for Savings. The objective is to also find a system/application that can interface with other applications/systems; e.g., Service Now that are used by the Bank.
  - b. Value:
    - i. Enhanced management of Business Continuity /Disaster Recovery Management information

- ii. Business Continuity Management System that can interface directly, other systems used by the Bank
- c. Risk of Not Implementing: Inability to provide services necessary for the growth and maturity of the BC/DR program.
- d. Technology Management Framework (TMF) Alignment: Non-Project Initiatives - 1C, 1E
- e. Category: Business Continuity/Disaster Recovery Management
- f. Tactical Implementation Plan:
  - i. Evaluate existing BC/DR Applications/Systems
    - 1. Meeting with vendors to evaluate their applications/systems
  - ii. Review information with senior management
  - iii. Present information to management for approval
- g. Target Start Date: 01/01/2023
- h. Target Completion Date: 12/31/2023
- i. Resources Required:
  - i. Internal: 2 (Existing Staff)
  - ii. External: 0
- j. Cost: \$50,000-\$100,000 year ballpark

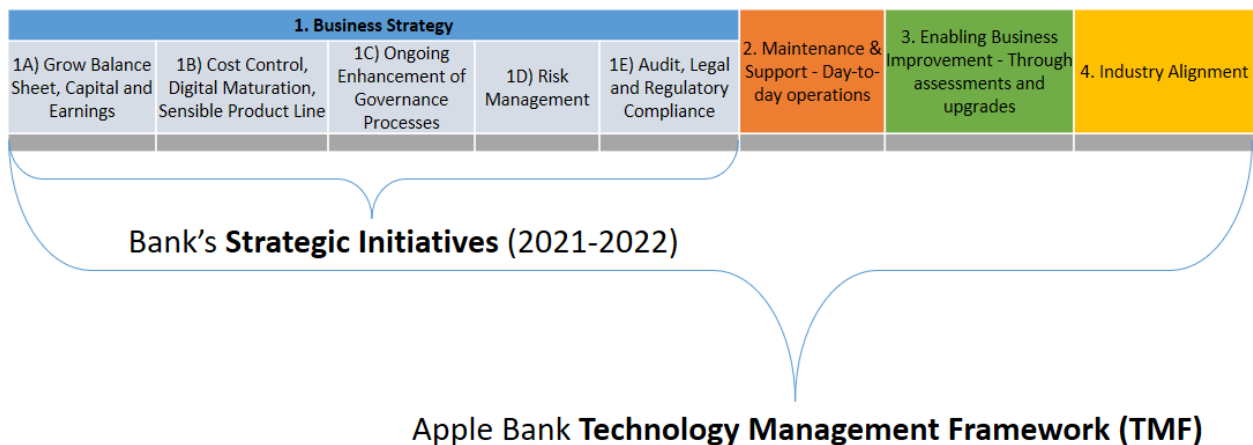
# Appendix 1: Technology Management Framework (TMF)



The Bank's Information Technology organization will align resources in the following four key areas:

1. Business Strategy – Aligned with the Bank's Strategic Initiatives
  - a. Grow Balance Sheet, Capital and Earnings
  - b. Cost Control, Digital Maturation, Sensible Product Line
  - c. Ongoing Enhancement of Governance Processes
  - d. Risk Management
  - e. Audit, Legal and Regulatory Compliance
2. Maintenance & Support – Day-to-Day Operations
3. Enabling Business Improvement – Through assessments and upgrades
4. Industry Alignment

Projects within this report will be tagged with one of the above categories to demonstrate alignment.





## Appendix 2: Budget

### Budget Estimates (2022): New Initiatives, Summary

Area	Budget	Annual Support
Enterprise Data Warehouse	\$1,506,000	\$373,500
Server Infrastructure	\$1,505,000	\$715,000
Network Infrastructure	\$4,630,280	N/A
Service Desk	\$689,000	\$1,615,000
Operations Quality Control	\$190,000	\$160,000
Digital Operations	\$842,000	\$31,000
Systems & Standards	\$372,000	N/A
IT GRC-CM & BCP/DR	\$100,000	N/A
Other – OPEX	\$120,000	\$55,000
<b>Totals</b>	<b>\$9,954,280</b>	<b>\$2,949,500</b>

### Individual Area Budget Plans

#### Enterprise Data Management - Enterprise Data Warehouse

Expense	Category	Q1	Q2	Q3	Q4
Contract Report/Extract Writers	Contractors	\$ 355,800	\$ 295,000	\$ 91,800	
Contract Data Modeler	Contractors	\$ 45,600	\$ 45,600	\$ 45,600	\$ 45,600
Contract Data Lineage / Part 504 (RC)	Contractors	\$ 60,000	\$ 20,000		
Contract ETL Developer	Contractors	\$ 60,000	\$ 20,000		
FIS BIC - Direct Access	Data		\$ 10,000	\$ 43,750	\$ 43,750
Analytics and Visualization - Tableau	Software				\$ 45,000
Data Catalog & DQ Tool - Collibra/Trillium	Software	\$ 44,375	\$ 44,375	\$ 44,375	\$ 44,375
SSIS third-party tools	Software	\$ 2,000	\$ 2,000	\$ 2,000	
Synthesizing, Masking tools	Software	\$ 3,000	\$ 3,000		
ER Studio Data Architect	Software			\$ 5,000	
Interfaces Build - Reason Consulting	Software	\$ 42,000	\$ 42,000		

## Infrastructure & Support

### Server Infrastructure

Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
Office 365 Including One Drive	Email and Chat Communication	\$ 110,000					\$ 900,000
Horizon VDI Deployment	Hardware and Computer Management	\$ 95,000					\$ 660,000
VxRail - Dev Environment	Server Storage and Compute			\$ 115,000			
Mobile Device Management (MDM)	Mobile Device Management				\$ 145,000		
Quantum On Premise Storage	Server Backup	\$ 60,000					
DMZ VxRail Cluster	Server Configuration	\$ 350,000					
VxRail Cluster Expansion	Server Configuration	\$ 600,000					
Microsoft Support	Server Support						\$ 40,000
Idera SQL Monitoring Software	Server Configuration	\$ 30,000					\$ 15,000

### Networking

Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
Wi-Fi Network including Cabling	Network	\$ 790,000					
IP Address Management (IPAM)	Network	\$ 150,000					
Isolated DMZ	Network	\$ 175,000					
Network Visualizer	Network	\$ 300,000					
Refresh EOL and Upgrade Devices for 10G	Network	\$ 525,280					
Software-Defined Wide Area Network (SD WAN)	Network				\$ 2,500,000		
RCC Network Engineer	Network						\$ 100,000
RCC Voice Engineer	Voice						\$ 90,000

### Service Desk

Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
EOL/EOS for Operating Systems (OS)	Software Asset Management					\$ 40,000	
CDI MSA Advanced Support	ServiceNow					\$ 144,000	
Core Conversion Initiative	Core Conversion Project						
PC Refresh	Endpoint Enhancement - BAU					\$ 500,000	
Secure Print Solution - PaperCut	Security Enhancement	\$ 5,000					\$ 24,000

### Quality Control

Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
Major Incident Management Module	ServiceNow				\$ 30,000		
Continuous Monitoring - TripWire Software	Continuous Monitoring	\$ 160,000					\$ 160,000
Service Now Developer - Contractor Resource	ServiceNow						

### Digital Operations

Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
Q2 Conversion Pre-engagement SOW w/ IBS	Core Enhancement			\$ 36,500			\$ 3,200
Q2 Integration with IBS (Main conversion)	Core Enhancement	\$ 208,000					\$ 12,000
Q2 Wire Integration with Finastra	Enhancement			\$ 50,000			\$ 12,000
FIS/D1 Online Account Opening w/ IBS	Enhancement						
FIS/D1 Online Account Opening Q2 Integration	Enhancement						
APB Customer to Customer Transfer	Enhancement			\$ 10,000			
RFP for New Online Banking Product	Enhancement	\$ 250,000					
VISA Integration w/ IBS	Core Enhancement	\$ 19,800		\$ 29,000			
ATM Activate Enterprise Upgrade	Upgrade	\$ 150,000					
Transition to Managed Card Services / Contactless	Enhancement			\$ 20,000			
C and I in Remote Lender	Onboarding	\$ 50,000					
Commercial Loans Data in EDW	Enhancement	\$ 12,000					
Build Secondary / Failover Connectivity for McCracken	Network Upgrade	\$ 6,700					\$ 3,800

## Systems and Standards

Expense	Category	Q1	Q2	Q3	Q4	OR Total
Role Based Access Software Implementation	Logical Access	\$ 350,000				
Cypress Upgrade	Logical Access	\$ 22,000				

## IT GRC-Change Management; Business Continuity/Disaster Recovery

Expense	Category	Q1	Q2	Q3	Q4	OR Total
CDI Work Effort for development/implementation	Software Asset Management					\$ 25,000
Replace/Enhance Incident Notification Solution	BC/DR Management	\$ 75,000				

## Other - All

Sub-Area	Expense	Category	Q1	Q2	Q3	Q4	OR Total	Annual Support
All	Training, Certifications and Conferences	Professional Development					\$100,000	
Business Continuity & Disaster Recovery Management	BC/DR Exercise - IT Infrastructure	DR Planning & Testing Enhancements					\$ 20,000	
Business Continuity & Disaster Recovery Management	Agility Recovery Planner (Current Software)	BAU						\$ 15,000
Server Infrastructure	Microsoft Support							\$ 40,000