Building a Robust Compliance Management System ("CMS") for Growing Mid-Size Level Bank

American Bankers Association Traditional Capstone Project

March 2024

Ivy Austria-Miller
Trustmark National Bank

Table of Contents

I. Executive Summary

Trustmark Bank is a commercial and financial services bank with $18 billion in assets and headquartered in Jackson, Mississippi. Trustmark operates 184 branches in Mississippi, Alabama, Tennessee, Florida, Texas, and a loan production office in Georgia. There is an appetite for Trustmark to explore options to expand its' Company footprint to neighboring states. However, as Trustmark continues to grow there is a bigger need to expand its compliance program. The proposed restructuring of Trustmark's Compliance Management System involves transitioning the program to comparable programs for mid-size level banks. Overall, the restructuring will provide for a more robust Compliance Management System that can better adapt to the changing regulatory environment, where regulatory scrutiny continues to increase.

The proposal will take a five phased approach, and the work will be conducted in-house through the establishment of working groups consisting of lines of business and compliance. These working groups will accomplish different tasks throughout the process allowing for: a more collaborative environment between the lines of business and compliance, direct involvement of implementation, engagement in the problem-solving process, and establishment of a better compliance culture. The five phased approach will take approximately four years to implement and the proposal to change the culture will take time to gain buy in from the lines of business, senior and executive management.

The four year roadmap will take into account the five phased approach which includes the following:

I. Phase I – Improvements to the vendor management, complaint management, and change management processes
II. Phase II – Buildout of lines of business controls which include: the quality assurance process, establishment of first line of defense Compliance Risk Management coordinators, key risk indicators (KRIs), and procedures
III. Phase III – Establishment of compliance culture across the Enterprise
IV. Phase IV – Compliance resource assessment which includes technology, staff, and training
V. Phase V – Implementation of the restructuring and renaming the department to Compliance Risk Management

Following the implementation, ongoing review, sustainability, and revision (when necessary) is important. For the restructuring to succeed, it must be continually reinforced from the executive level downward once implementation is completed. Also, metrics need to be established to evaluate the success and effectiveness of the newly restructured Compliance Management System. These key risk indicators need

to measure the growth, understanding from the lines of business, the lines of business effectiveness in management controls relative to compliance, and compliance receiving satisfactory ratings from internal audit, and regulatory exams. Compliance metrics will come from many potential sources to include: culture surveys, risk assessments, disclosures, focus groups, compliance hotline, etc.

The largest cost drivers of this endeavor will come from the potential of adding personnel, implementing new technology, and investing in ongoing training. The approximate estimated overhead cost for the propose restructuring is $3.958 million for implementation. While this endeavor is costly to the Bank, this estimated cost can be reduced through the exploration of automation, cross training employees, utilizing existing technology and making enhancements. These factors will be exhausted prior to considering adding resource costs to the organization.

Implementing organizational change will take time and will be met with resistance especially with the current culture in the Bank. While compliance is not new to the organization, there are a few hurdles that were identified. This includes: resistance to change, inability to resource, and potential knowledge gaps. An important element in overcoming the challenges is the delivery and approach in communication and creating a collaborative environment. This is central to aligning Fair and Responsible Banking and Compliance (FRBC) and 1 Line of Defensive (LOD) towards a common objective. Additionally, the ability of open dialogue can play a vital role in overcoming challenges and building a strong compliance baseline. Overall, communication and collaboration are key to overcoming these challenges.

The proposal will not only address the need to expand Trustmark's compliance program but will improve processes across the organization for the lines of business and compliance, establish a better collaborative culture, and position the bank to better comply with applicable laws, regulations, and industry standards. Furthermore, the restructuring will help to prevent unethical or inappropriate behavior by employees, better detect reporting of failures, and mitigate the risk associated with noncompliance. In addition, the proposal will provide positive impacts that include: mitigating risks of compliance violations, increased transparency and accountability, and improved corporate governance, by protecting and minimizing reputational risk, and increased employee morale. The implementation of an effective Compliance Management System is essential for Trustmark' regulatory well-being and the Bank's commitment to doing the right thing.

II. Introduction and Background

Trustmark Bank transitioned from a small to a mid-size level bank on December 31, 2013, when it crossed the $10 billion threshold and became a bank with an asset size of $11.79 billion. In comparison Trustmark Bank had $18.72 billion in assets at the end of 2023 Trustmark continues to grow, and for the fiscal year ending on December 31, 2022, Trustmark Bank had $18.01 billion in assets. Trustmark Bank intends to grow its asset size to $30 billion in the next few years through expanded into different markets and offering new products and services in its Company footprint.

The current Compliance Management System ("CMS") program is becoming inadequate for the Bank's size, and there are areas in the program that can be improved. Additionally, there are new processes that need to be developed to ensure Trustmark has appropriate Compliance coverage.

1. CMS is the method by which a bank manages consumer compliance risk. An effective CMS ensures compliance with consumer protection-related laws and regulations, and it proactively detects and prevents of consumer harm. A bank should develop and maintain an effective CMS Program that is appropriate for the size, complexity and risk profile of its operations. A bank's overall CMS includes policies, procedures, processes, monitoring, and testing programs, and a compliance audit function which tests compliance with all applicable laws and regulations.[1] An effective CMS program will maintain the following components and subcomponents.[2]Assessment and Management of Compliance Risks:
    a. Act as compliance subject matter experts on projects and committees
    b. Evaluate the development of, and changes to, products, services, processes, and systems to determine compliance risk and impacts, and ensure policies remain complaint
    c. Provide compliance support to internal and external parties (e.g., answer questions, review marketing and external communications, conduct research and analysis)
    d. Review and/or provide compliance training to applicable parties
    e. Participate in conducting due diligence for vendors
    f. Design and maintain a comprehensive compliance risk assessment program to identify and mitigate risk within the organization's risk appetite

[1] Comptroller's Handbook CC-CMS Compliance Management Systems Version 1.0, June 2018. https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/compliance-mgmt-systems/pub-ch-compliance-management-systems.pdf

[2] American Bankers Association CRCM Online Prep Course

g. Conduct compliance risk assessments in accordance with the risk assessment program to evaluate relevant information and communicate results to applicable parties

2. Compliance Monitoring
    a. Define the scope of a specific monitoring or testing activity
    b. Test compliance policies, procedures, controls, and transactions against regulatory requirements to identify risks and potential exceptions
    c. Review and confirm potential exceptions, findings, and recommendations with business units and issue final reports to Senior Management
    d. Validate that any required remediation was completed accurately and within required timelines
    e. Administer a Complaint Management Program
    f. Review first line compliance monitoring results and develop an action plan as needed
    g. Evaluate the reliability of systems of record and the validity of data within those systems that are used for compliance monitoring
3. Governance and Oversight
    a. Establish and maintain a Compliance Management Policy to set expectations for Board, Senior Management, and Business Unit Responsibilities
    b. Develop, conduct, and track enterprise-wide and/or job specific compliance training
    c. Conduct periodic reviews of the Compliance Management Program to evaluate its effectiveness and communicate results to appropriate parties
4. Regulatory Change Management
    a. Monitor and evaluate applicable regulatory agency notifications for new compliance regulations or changes to existing regulations and assess potential regulatory impacts and remediation needs
    b. Assess new, revised, or proposed regulatory changes for compliance impacts, communicate to appropriate parties, and develop action plans as needed
    c. Assess regulatory guidance and compliance enforcement actions to determine if remediation is required to address potential compliance impacts
    d. Report on the status of regulatory changes and implementation to appropriate parties
    e. Monitor and validate action plans for confirmed regulatory impacts to ensure timely adherence to the mandatory compliance dates
5. Regulatory and Auditor Compliance Management

a. Prepare and review requested audit/exam materials to ensure timely and accurate fulfillment and self-identify potential areas of concern
b. Participate in audit/exam meetings to provide business overviews, address questions, discuss findings, and/or provide updates to appropriate parties
c. Review and draft responses to audit/exam results and ensure action plans are developed and communicated to appropriate parties
d. Report on Action Plan Status to appropriate level of management and auditors/examiners
e. Coordinate and submit ongoing regulatory reports to auditors/examiners

6. Compliance Analysis and Internal/External Reporting
    a. Analyze and validate data to support regulatory reporting and ensure accuracy and comprehensiveness
    b. Complete required reporting, ensure timely submission to the appropriate agency, and resubmit when required
    c. Develop, implement, and monitor a plan of action to prevent future reporting errors or breakdowns

Trustmark's CMS program is comprised of eight pillars that are grouped into two primary functions: Board and Management Oversight and Compliance Risk Management Program. Board and Management Oversight is comprised of: Board Oversight, Regulatory Change Management, Risk Assessment, and Issue Management. The Compliance Risk Management Program is comprised of: policies and procedures, training, testing, and consumer complaint resolution. The following section outlines Trust Mark's current state for each of these pillars and their functions.

Board and Management Oversight

- Board Oversight – The Board supports Trustmark's CMS by ensuring compliance resources are commensurate with the Bank's complexity and risk profile. These resources include systems, capital, and human resources. Additionally, the Board ensures that compliance staff is knowledgeable and given enough authority to achieve compliance risk management goals. The Board also engages in the Bank's CMS through the approval of policies, establishing the compliance risk appetite, and providing overall strategy for the program's execution. The Board is made aware of emerging or changing compliance risks through the escalation of issues, compliance reporting, monitoring and testing results, and other information elevated through the Bank's governance process.

- Regulatory Change Management – Regulatory Intelligence is responsible for monitoring and tracking the enterprise-wide legislative and regulatory compliance changes and provides reporting into the governance process. The Regulatory Intelligence process identifies laws and regulations applicable to the Bank's activities and allows the Bank to stay abreast of evolving regulatory requirements. Management manages the process, which includes responding in a timely manner to applicable regulatory changes to the Bank. Management reviews Regulatory Intelligence reports, applicable committee meeting minutes, adopted policies and procedures related to the change, and monitoring or auditing reports for reviews conducted throughout and after the change. Management will monitor regulatory developments to identify and communicate to staff upcoming changes in applicable consumer protection-related laws and regulations. In addition, Management will take appropriate steps in advance of changes to prepare the Bank to respond to changes once they occur and review the change after implementation to determine that actions taken achieved the planned results. Management will also communicate to customers as needed, including timely issuance of any required disclosures or account agreements.
- Risk Assessment – Compliance is responsible for developing, maintaining, and performing consumer compliance risk assessments. This process identifies, measures, and monitors consumer compliance risks by line of business for each applicable regulation. In addition, the consumer compliance risk assessment process uses the same risk rating methodology as the Enterprise Risk Management Department for consistent interpretation of risks across the enterprise. Each risk assessment is entered into the governance process when completed, and a report for all consumer compliance risk assessments will be entered into the governance process annually. The risk assessment process is vital to the execution of the Bank's CMS as it informs other risk-based decisions such as the creation of the annual testing schedule. As such, this process is highly collaborative with the lines of business and members across the Compliance Department are engaged in the risk assessments execution.
- Issue Management: The Director of Consumer Compliance is responsible for the oversight of the Issue Management process, however, members across FRBC are responsible for its timely and effective execution. Trustmark utilizes Archer as the tool to centralize the logging, tracking, remediation, and validation of compliance issues identified across the Bank. Findings are identified and managed by the following teams: Audit, Model Risk, SOX Compliance, Vendor, Enterprise Risk, Information Security, Corporate Security, Wealth Management, Legal, Fair Lending, BSA, CRA, Asset Review, the Regulatory Compliance and Mortgage Compliance programs. The listed teams

are responsible for overseeing and providing guidance to the make sure all findings are properly addressed, and the assigned business team member is the true owner of the finding and is responsible for remediating the finding in a timely manner and providing periodic updates on the status of remediation. The compliance team member responsible for oversight and timely closure of the remediated issue is the Reviewer.

Compliance

- Policies and Procedures: New compliance policies are developed, and existing policies are revised as regulatory, investor and/or procedural changes occur. Policies primarily focus on regulatory compliance including, but not limited to: Retail Banking, Mortgage Quality Control ("MQC"), Fair and Responsible Banking ("FRB"), Community Reinvestment Act ("CRA"), Bank Secrecy Act ("BSA")/Anti-Money Laundering (AML) and Wealth Management. The Compliance Committee has the authority to approve policies based on the Policy on Policies. Once approved, compliance policies are located on Trustmark's internal website, and in the Compliance Policy Manual, making policies easily accessible to all business units and associates.
- Compliance Training: Compliance training is an integral part of our Compliance Risk Management Program. Compliance training is done in conjunction with the Organizational Development and Training Department, which facilitates formal webcasts and computer-based training in response to compliance training needs. Webcast training includes sessions from major compliance training vendors and sessions designed by the Organizational Development and Training Department. Compliance training needs may be determined based on required, annual regulatory training and based on risks identified through Internal Monitoring, Risk Assessments, Regulatory/Legislative Change Management, or identified through complaint analysis. Directors, Sr. Risk and Compliance Managers and reporting managers also identify training needs through ongoing tracking of regulatory changes and participation in working groups, which implement those changes into the operating environment. Once training needs are identified, the FRBC Department determines what operational areas are affected and works with the Corporate Training Department to finalize training needs. The Corporate Training Department develops a formal, annual schedule for associates in conjunction with Directors and Sr. Risk and Compliance Managers to assign necessary training and audience participation for the identified training needs. The Organizational Development and Training Department has a central system to track the progress of completion for associates assigned to a specific training activity (webcast/CBT/classroom). Associates are held

accountable for completing the training through a mandatory requirement for completing all assigned training.

- Compliance Testing: The Bank monitors regulatory compliance progress toward goals for the enterprise. Each line of defense plays a role in the Bank's approach to compliance monitoring and testing.
    - First Line of Defense - Business lines perform quality control and quality assurance testing and monitoring of business line processes and controls they manage using a risk-based approach, which may include control performance and potential indicators of regulatory compliance risk.
    - Second Line of Defense - FRBC monitors the adequacy and effectiveness of the Bank's regulatory compliance controls. Regulatory compliance is addressed through second line monitoring/ testing for regulatory compliance and execution of risk assessments.
    - Third Line of Defense - Internal Audit is responsible for independently evaluating the effectiveness of this Program and the design and effectiveness of regulatory compliance controls across the enterprise. Internal Audit findings may also inform Compliance of monitoring and testing activities.

  Compliance testing and monitoring is the process of independently evaluating adherence to internal policies and procedures, laws, and regulations. Compliance Testing of activities performed within the lines of business is independently conducted by the FRBC teams – Consumer Compliance, Mortgage Quality Control, Fair Lending Analytics, Regulatory Reporting, and the consumer compliance risk assessment teams. Compliance monitors, risk, adequacy, and the effectiveness of the Bank's controls and consistency with regulatory requirements. Issues arising out of the compliance program are managed in accordance with the Company Policy and the Compliance Archer Issues management procedures.

- Consumer Complaints: The complaint process is governed by the Complaints Management Policy. The lines of business are responsible for logging, investigating, and resolving complaints received in their respective areas. In addition, the lines of business are responsible for responding to all complaints and should coordinate with Strategic Initiatives Manager for Compliance and Risk and/or the Sr. Fair Banking Manager for responses to heightened risk complaints as determined by the line of business or the Complaint Working Group. The day-to-day activities of monitoring and managing the enterprise's platform (RSA Archer) resides with the Strategic Initiatives Manager

for Compliance and Risk, which monitors the collection of complaints including third-party complaints. The Complaint Working Group meets monthly with representation from various risk specialists to monitor complaints for instances of Unfair, Deceptive, Abusive Acts and Practices ("UDAAP"), fair lending concerns, violations of law, or sales practice concerns. A report is provided for entry into the governance process on a quarterly basis of the findings of the working group.

Deficiencies in the Trustmark's CMS program

When comparing Trustmark's CMS program to industry standards and regulatory requirements, the CMS program has identified deficiencies related to Vendor Management, Change Management, Compliant Management, Compliance Governance and Oversight, and the Compliance Structure. The details of the deficiencies in each area are provided below.

I. Vendor Management – The Compliance Department is conducting a risk assessment review for new vendors prior to onboarding but there is no ongoing due diligence being conducted for vendors that are rated as having high Compliance risk. This is a regulatory requirement to ensure that vendors are staying compliant with regulatory expectations and that executive management is informed of vendors who are not compliant.

II. Change Management – The Compliance Department is only keeping track of the regulatory changes. Also, the CMS program has treated the Regulatory Intelligence process and the Change Management process as two separate processes, when in fact, they are the same process. Additionally, there are two other pillars that are not taken into account; they are: products and services and technology changes. Evaluating and updating product offerings and business strategies is critical to a financial institution's success. Financial institutions want to be responsive to evolving consumer needs and expectations and be positioned to enter new markets and product areas to further their strategic plans. Finally, it is important to highlight the significance of managing information technology changes at financial institutions, such as system conversions. Because most financial institution operations and internal controls are based on automated systems, appropriate management of technology updates and changes can help keep the institution running smoothly and compliant with laws and regulations. It is important to work with vendors to effectively implement changes.[3]

[3] Consumer Compliance Outlook. Promoting Effective Change Management. https://www.consumercomplianceoutlook.org/2019/second-issue/promoting-effective-change-management/

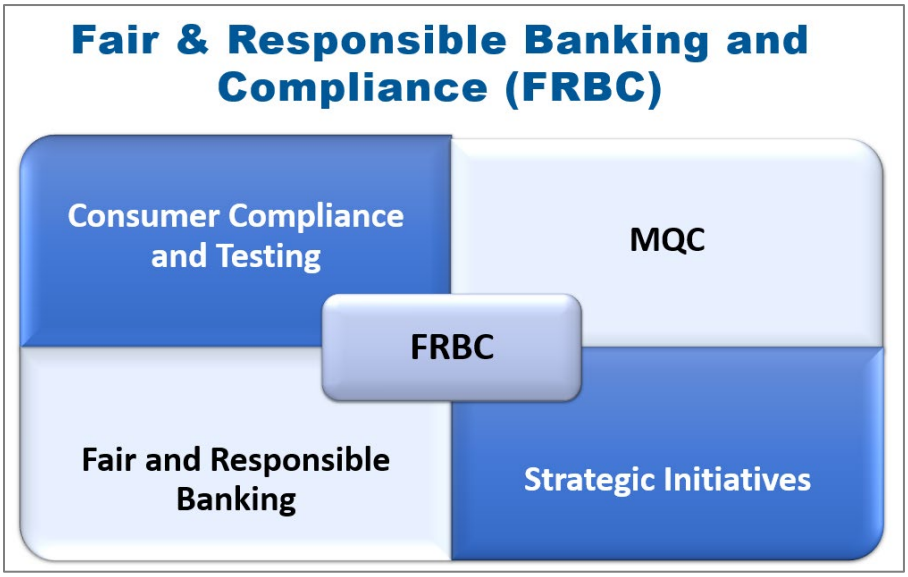
III. Complaint Management Process – The lines of defense complaint handling confirms that certain controls are in place, but 1LODcontrols (departmental guidelines, procedures, and QA processes) are not documented to fully inform associates of their responsibilities and accountabilities for execution of obligations to assure a well-functioning control environment. Additionally, management should continuously reinforce during the normal course of business meetings the importance of capturing all complaints, continue to implement automated processes to identify complaints, and identify missed opportunities for not logging complaints. Trustmark continues to show a low volume of complaints and may be subject to criticism for ineffective processes. The contributory causes to these findings include: 1) lack of continuous training and reinforcement; 2) lack of documented guidelines and procedures; 3) lack of complaint intake channels; and 4) no established QA monitoring program to self-identify errors.

IV. Compliance Governance and Oversight – The Compliance Testing and Consumer Compliance Advisory responsibilities are both incorporated into the Compliance Testing group. According to regulatory expectations, the Compliance Testing group needs to be independent of consumer compliance advisory to the lines of business. There is a contradiction in function and potential for bias by having both functions in the same area. Additionally, there are not multiple subject matter experts in the Compliance Advisory area but only one person in the group who is knowledgeable in all compliance regulations; meaning the ability to articulate how laws, regulations, and guidelines are relevant to 1LOD business processes and provide guidance to build controls to mitigate any potential risks.

V. Compliance Structure – In the current state, the Compliance Department is structured as follows:

This structure was created to address regulatory issues that occurred from 2013 to present and when Trustmark was considered a smaller size bank. However, since Trustmark is now deemed a mid-size level bank (defined as a bank with an asset size of $10 billion and over) and has plans to double in size, the Compliance Department needs to be restructured in order to ensure it continues to meet the regulatory demands.

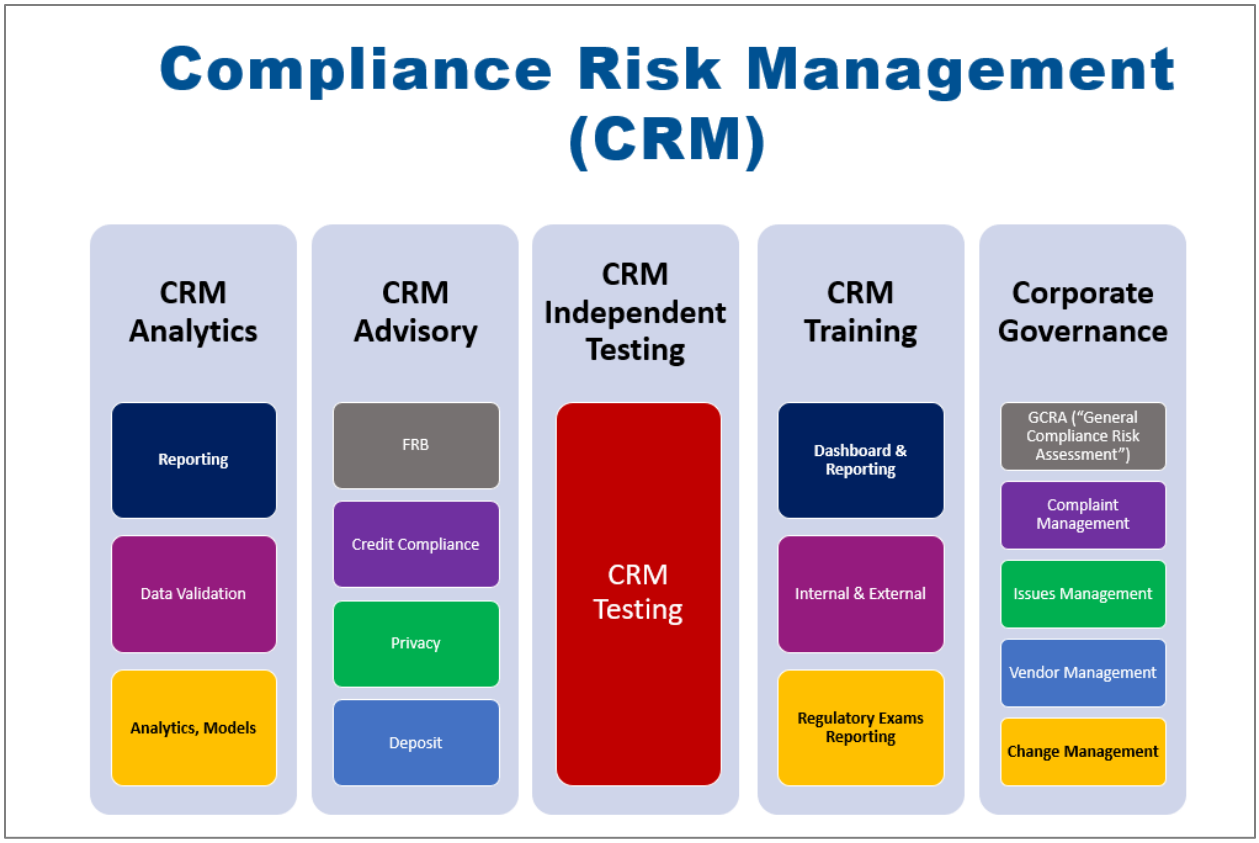
CMS Restructuring



The proposal is to take the existing CMS program and transform Trustmark's CMS program using a phased approach to complete this transition. This will include the following:

1. Addressing the deficiencies in Vendor Management, Change Management, Complaint Management, and Compliance Governance and Oversight
2. Building out additional workflow processes in the lines of business and Compliance
3. Developing a better Compliance Culture across the organization
4. Restructuring FRBC to the new Compliance Risk Management structure

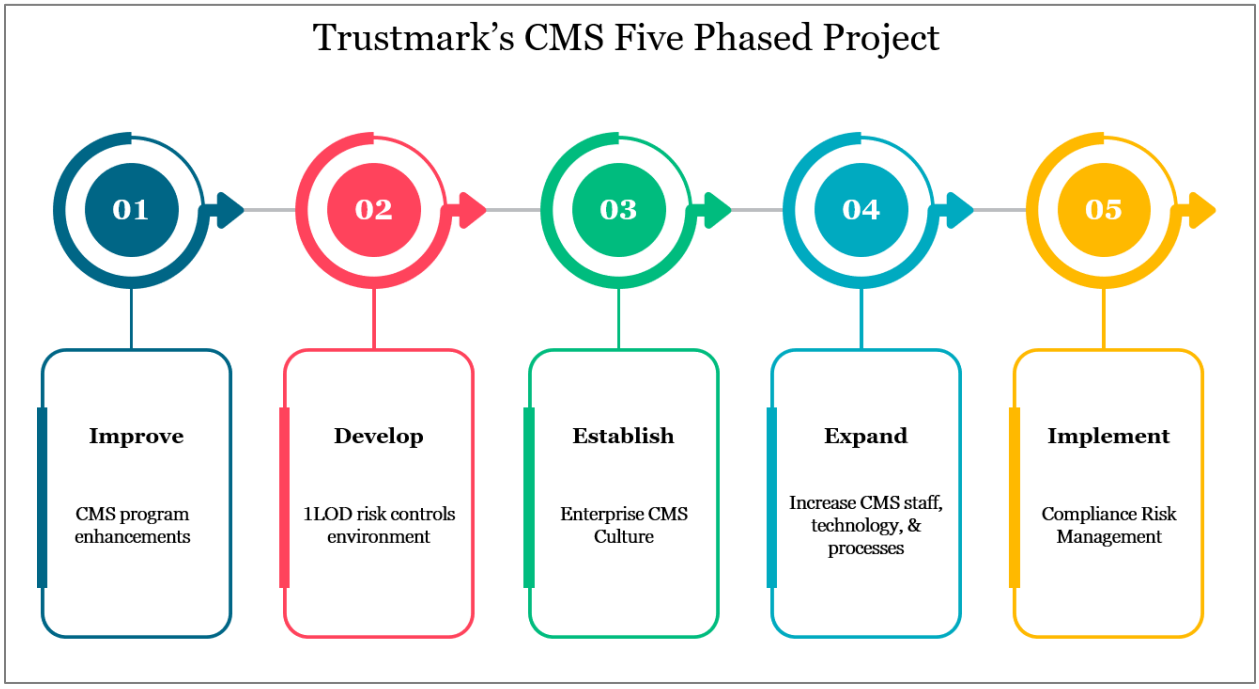
When the transition is completed the Compliance Department will have the following structure:



This restructuring will provide for a more effective CMS program for Trustmark and better position the Bank to be able to handle increasing regulatory demands. The strategic plan for this initiative is provided in the following sections.

III. Strategy and Implementation

The Compliance Risk Management restructuring will take a phased approached that consists of: 1) improving existing CMS processes, 2) buildout of lines of business controls which includes: quality assurance (QA) process, establishment of first line of defense ("1LOD") Compliance Risk Management ("CRM") coordinators, key risk indicators (KRIs), and procedures, 3) establishment of CRM culture across the enterprise, 4) CRM staff and resource assessment (employees, technology, workflow processes, etc.), and 5) restructuring of the current CMS program. The diagram below illustrates Trustmark's CMS five-phased project.



Prior to the implementation of the phased approach a discussion with executive management and the Board is needed to gain approval of integrating the organization's strategic plan of expanding compliance. Once approval has been provided the phased approach can begin. The details of each phase are provided in the following sections.

IIIa. Phase I – Improvement of current CMS program

As mentioned in the previous section there were a number of deficiencies that were identified in the vendor management, change management, compliant management, compliance governance & oversight processes that needed to be addressed prior to the restructuring. There is current work that is taking place

in each of these areas and is expected to be completed by the end of 2025. The following summarizes the strategic plan for each process.

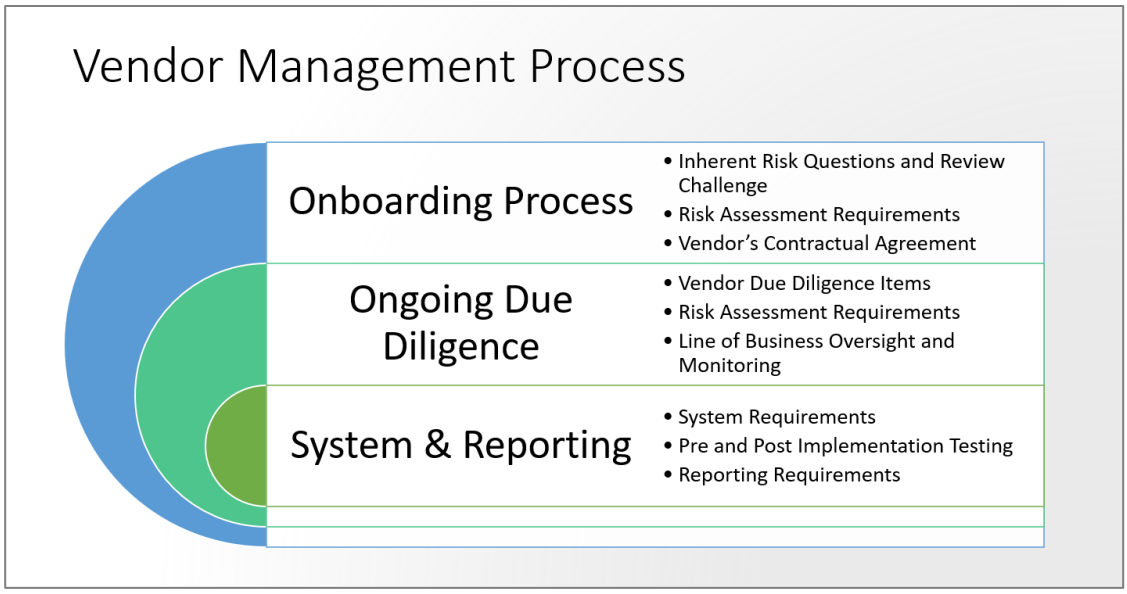
a) Vendor Management – The Vendor Management process is owned and managed by Enterprise Risk Management ("ERM"). ERM has an established Vendor Oversight Policy that defines the types of vendors which require oversight (Source: OCC 2017-43). Vendors can be used to offer new, modified, and expanded products and services as noted below:
    - **New** products and services may differ substantially from previous bank offerings and may result from relationships with third parties. New products and services include those offered for the first time, as well as offerings that the bank previously discontinued but will offer again after a substantial period of time has passed. New products and services can provide entrance into or solutions for new financial markets, add new convenience and capabilities for customers, or assist in managing risks for customers.
    - **Modified** products and services differ substantially from existing products and services in nature, terms, purpose, scale, or use. Modified products and services substantially alter the underlying risk qualities or characteristics of the existing products and services.
    - **Expanded** products and services are those offered beyond a bank's current customer base, financial markets, venues, or delivery channels.

The Vendor Management Process consists of three channels:

1) Vendors that offer new products, and services that do not require approval from New Products and Services Committee (NPSC): These are vendors that do not meet the definition set forth by ERM Vendor Management Policy. Examples include: HR vendors for benefits to employees, Consulting services for Bank purposes, etc.
2) Vendors that offer new products, and services that do require approval from NPSC: These are vendors that meet the definition set forth by ERM Vendor Management Policy.
3) Vendors who are up for renewal of their contracts with Trustmark (Renewals do not require reapproval from NPSC.)

The regulatory agencies have released new guidance on vendor management as of June 6, 2023; as a direct result of this, ERM is revamping the Vendor Management process to meet the regulatory demands. In addition, there has always been a regulatory expectation for FRBC to conduct due diligence reviews on vendors that are conducting transactions, marketing, sales, etc. on behalf of the bank. The due diligence

reviews must be completed prior to and after onboarding. ERM and FRBC have partnered together to develop a more robust due diligence process and create a more collaborative environment between the two groups. The chart below illustrates the FRBC controls that will be established in order to ensure a sound and robust vendor management process.



- In the onboarding process, FRBC needs to develop inherent risk questions that are provided to the vendor to determine whether or not they require compliance oversight. Vendors who are acting on activity on behalf of the Bank (i.e., marketing, payment activity, etc.) and/or conducting banking services (i.e., deposits activity, loan activity, etc.) on behalf of the Bank's customers will generally have compliance applicability. Inherent risk questions are structured to trigger FRBC review depending on how the vendor answers the questions. For example, Yes/No questions will trigger FRBC review if the vendor answers "Yes" to any of the questions. In order to prevent vendors from answering questions in a way to avoid compliance oversight, a Review Challenge is built into the process where FRBC reviews vendor responses. The Review Challenge gives FRBC the authority to challenge vendor responses and indicate whether the vendor has compliance applicability. The vendors who have compliance applicability will be subjected to a vendor risk assessment. FRBC will establish a set of criteria that will be utilized in the risk assessment and develop procedures outlining the process. The risk assessment determines the level of risk associated with the vendor, which is then presented to the lines of business to determine whether they want to continue with the onboarding of the vendor or consider another vendor. The risk rating determines the vendors who will be subjected to a more rigorous due diligence (i.e., high risk vendors will be subjected to a more in depth review versus low risk vendors who will be subjected to a lighter review). At the

conclusion of the risk assessment, FRBC will work with Legal to determine the due diligence items that the vendor has to provide for the ongoing due diligence reviews (The list of due diligence items will be an Appendix in the contract.). For example, a vendor who has UDAAP applicability will be required to provide monthly complaint reporting to the Bank. In addition, the vendor will be required to have controls in place to ensure they are compliant with the rules and regulations applicable to the Bank. The lines of business will be responsible to collect this information from the vendor and review the complaint report to ensure that it has all the information FRBC is needing for their review. Lastly, FRBC will need to establish documentation requirements to track the onboarding process.

- In the ongoing due diligence process, FRBC will conduct periodic risk assessments of the vendors that have compliance applicability. The lines of business will be responsible for collecting the due diligence items from the vendor and reviewing the documentation. FRBC will be developing criteria for the risk assessment for the ongoing due diligence process. The objective of the risk assessment is to ensure that the vendor is compliant with applicable rules and regulations that apply to the Bank, and that they are treating the Bank's customers consistently. Additionally, the review will validate whether the lines of business have the appropriate oversight and monitoring of the vendors. Vendors who carry high risk may result in contract terminations if they are not complying with the Bank's rules and with applicable regulations. Lastly, FRBC will need to establish documentation requirements to track the ongoing due diligence process.
- FRBC will work with ERM to implement a Vendor Management System that will keep track of the onboarding and ongoing due diligence processes. This will provide transparency into the reviews being conducted at the enterprise level and create awareness of the vendors that pose higher risk. ERM and FRBC need to establish system requirements to ensure that the system has the functionality needed to carry out specific processes. Secondly, ERM and FRBC need to conduct pre and post implementation testing to ensure that all bugs and issues are identified to ensure that the data is accurate, and the system is performing as intended. Lastly, ERM and FRBC need to ensure that the system is able to meet reporting requirements for internal and external exams, and for executive/senior management reporting.

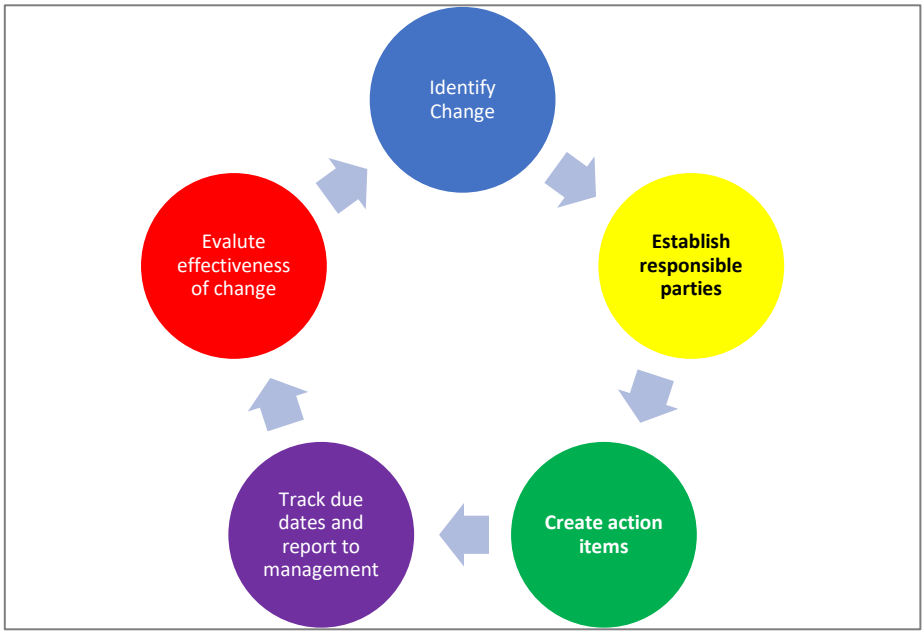
b) Change Management

The next area that needs to be improved upon is change management. As mentioned in the previous section, in the current state the only aspect that has been taken into consideration is regulatory intelligence. Change management is one of the assessment factors under the Federal Financial Institutions

Examination Council (FFIEC) Consumer Compliance Rating System. The change management process is an essential pillar of an effective CMS Program. The Bank's change management process needs to have established components in order to be effective. The benefits of an effective change management process are:

- Enterprise awareness of the current and projected regulatory environment
- Identifying opportunities and offering guidance during times of product and process development
- Potential enhancements to the design of workflow processes supporting compliance with regulations, laws, and industry best practices
- Enhancing compliance oversight of the lines of business ("LOBs") responsible for carrying out processes
- Increased knowledge of regulatory matters to aid internal associates
- Increased knowledge of financial industry changes and initiatives with regulatory focus
- Mitigating risk and/or potential harm to the organization and/or its customers, etc.

An effective change management process involves a timely and adequate management response to changes in applicable laws and regulations, market conditions, and products and services offered, by evaluating the change and implementing responses across impacted lines of business. Also, the change management process includes evaluating products and service changes both before and after implementing the changes. The following diagram outlines the components of the change management process that FRBC will be using to develop their process:



The first component of the change management process is to monitor change and the associated risks to the Bank. This includes:

- Identifying statutory/regulatory changes that ***affect*** the Bank's operations
- Determining how changes to the Banks's products, services, and technology would ***impact*** the Bank's consumer compliance obligations

The second component of the change management process is to establish responsible parties. The following provides the responsibilities for each area:

i. Executive Management

a. Determine whether the proposed product/service aligns with the Bank's strategic direction.

b. Determine the risk(s) of the proposed product/service and whether management will accept or reject the associated risk(s).

ii. First Line of Defense ("1LOD")

a. Determine how changes (i.e., regulatory, product, services, and/or technology) to the institution's products, services, and technology would impact the Banks's consumer compliance obligations.

b. Evaluate the costs and benefits to both the Bank and its customers. The new products/services should not benefit the Bank at the expense of its customers.

c. Evaluate the Bank's capacity to make the change, including the costs to implement the change, and whether the Bank has the necessary expertise or if third parties need to be engaged.

d. Develop action plans and reporting to executive management.

e. Engage FRBC in ongoing conversations to ensure changes meet consumer compliance obligations.

f. Develop checklists.

g. Update policies, procedures, customer facing documentation as needed, and develop training for staff as appropriate. As well as obtain approval from FRBC prior to implementation of documentation and training.

h. Conduct pre and post implementation testing as appropriate.

iii. Second Line of Defense ("2LOD")

- **a.** Monitor regulatory changes and the associated risks to the Bank and inform 1LOD of regulatory changes that have FRBC applicability.
- **b.** Provide guidance to the 1LOD and review lines of business documentation.
- **c.** Participate in pre and post implementation validation testing.
- **d.** Adjust 2LOD policies, programs, and procedures, if necessary.
- **e.** Adjust risk assessment and testing protocols, as necessary.
- **f.** Evaluate training needs for the enterprise.

The third component of the change management process is actions items. Actions Items should include the following components:

- Research the change (beyond any strategic factors already considered)
- Evaluate the impact on specific processes (including software and vendors)
- Develop action plans and document responsible parties
- Develop checklists
- Update policies and procedures as needed, and develop training for staff as appropriate

Testing the implemented change prior to the change going live is critical. This is particularly important when changes involve technology, to ensure the functionality, customer facing documentation, and disclosures correctly capture the Bank's practices and related regulatory requirements.

The fourth component of the change management process is reporting to management. It is important that due dates are established and tracked. Also, it is important that an approval process is established, and appropriate signoff is conducted for each step. Lastly, it is important that approvals and the progress of actions plans are documented and reported.

The last component of the change management process is evaluating the change. Post implementation testing should be conducted by the 1LOD and 2LOD to ensure that the changes were effectively implemented. Also, any identified weaknesses will include a corrective action by the 1LOD to ensure the weaknesses have been addressed appropriately.

I. Complaint management program

An effective complaint management process should include the following elements:

a) The nature or number of substantive complaints from consumers indicates potential CMS weaknesses
b) Consumer complaints that raise legal issues involving the following must be categorized and escalated (including to Senior Management and to the Board):
    - Potential consumer harm from UDAAP or discrimination, or other "significant consumer harm"
    - Unauthorized product enrollment
    - Account openings or upgrades (including addition of ancillary products)
    - Improper sales practices
    - Imminent foreclosures, or
    - Other regulatory compliance issues
c) Management must monitor for consumer harm and CMS deficiencies
d) Complaints must be resolved promptly and completely
e) The program should include root cause analysis. Results of root cause analysis should guide corrective action, including modifying policies, procedures, training, monitoring, and/or other appropriate business adjustments
f) Where appropriate, consumer complaints may result in retrospective corrective action to correct negative effects to consumers based on the Bank's actions
g) Remediation practices should include consideration as to whether all harmed consumers have been remediated

II. Compliance Governance and Oversight

As mentioned in the prior section, FRBC conducted a gap analysis of the Complaint Management process to validate whether these elements were being incorporated. There were several deficiencies identified with lines of business and FRBC. The following outlines the action plan to remedy these deficiencies. It should be noted there is already work that is being conducted to correct these deficiencies.

1) 1LOD complaint handling processes and procedures need to be developed. Departmental guidelines should consider:

a) Relevant information from the Corporate Complaint Policy.

b) The frequency and number of times a customer should be contacted if attempts fail to reach the complainant.

c) The type of contact that will be used (phone, mail, email) and under what circumstances the type of contact will be used.

d) A description for complaint intake.

e) LOB accountability and responsibilities for complaint investigation and resolution (particularly that all the issues noted in the complaint require explanation or response to the customer).

f) Standards for professional response.

g) Time constraints to complete the investigation and complete the response.

h) Quality Assurance ("QA")/Quality Control ("QC") process to review associate responses.

i) Escalation procedures when complaints potentially indicate a legal, fair lending, UDAAP, sales practice or systemic issues.

j) Clear identification of the root cause for the complaint.

2) 1LOD Management should -

a) Periodically reinforce the importance of complaint capture and investigation requirements with their teams.

b) Maintain up-to-date departmental procedures and oversight of associates completing complaint investigations

c) Consider partnering with FRBC to assist in development of internal processes.

d) Consider a central 1LOD point of contact for enterprise complaints.

3) 1LOD should consider the potential for implementing a mechanism for customers to independently submit complaints directly to the Bank electronically and once implemented provide access information on customer facing communications.

4) Although annual employee compliance training is provided, departmental complaint management training should be enhanced to include the following:

a) Communicate the importance of logging complaints, which includes: when to log a complaint, and the criteria needed to log a complaint.
b) The objective of the consumer complaint process.
c) Consequences of a non-effective complaint program.
d) How Trustmark defines a complaint.
e) Complaint management roles and responsibilities.
f) All associates should receive thorough training.

5) FRBC should enhance existing job aids that are outlined in recommendation #4.

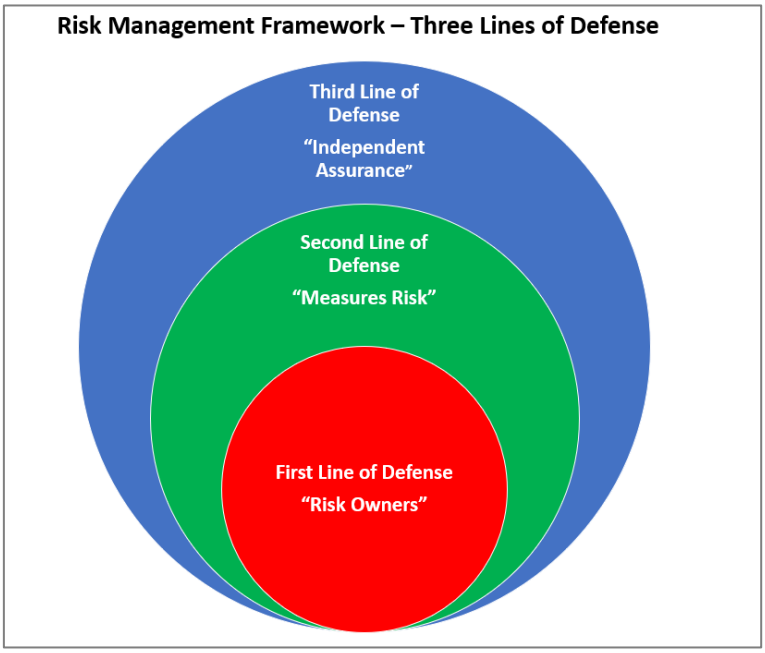
6) FRBC should enhance the Consumer Complaint Policy and Procedures to promote understanding of what is considered a complaint and outline the responsibilities and roles of 1LOD and FRBC.

7) A partnership between FRBC, Business Unit Risk Coordinators ("BURCS"), and 1LOD Management should be implemented to develop a cohesive strategy that informs and educates associates on an on-going basis on the recognition of a complaint, what constitutes a complaint, the risks associated with a complaint, and the escalation of a complaint.

The 1LOD will designate a point of contact who will be responsible for establishing the Complaint Management working group and develop a project plan to address the deficiencies stated. Furthermore, FRBC will be a participant in the working group and provide regulatory guidance, and approvals of departmental guidelines, procedures, and QA processes. Additionally, FRBC will enhance the complaint management policy, procedures, training, and job aids to include a clearer definition of a complaint and define the roles and responsibilities of each line of defense (1LOD and FRBC). FRBC will participate in the complaint management working group to assist the 1LOD in addressing the deficiencies in their control environment.

IIIb. Phase II – Development of 1LOD risk controls environment

In order to understand this phase, it is important to briefly discuss the risk management framework. An effective risk management framework has three lines of defense, for each line of defense there needs to be risk governance to support and provide oversight to the framework. The three lines of defense is a standard model for banks in managing uncertainty and mitigating downside risks. The following diagram provides the three lines of defense and the function for each line of defense.



1. The first line of defense consists of frontline staff, this is often referred to as customer facing employees who have direct/indirect interaction with customers. They are the risk owners in this model.
2. The second line of defense is created by the oversight functions made up of ERM and Compliance. These functions set and monitor adherence to policies and oversee the first line with regard to risk and compliance. The second line measures the risk and communicates this risk to the risk owners, who determine whether they will accept the risk or mitigate the risk.
3. The third line of defense is Internal Audit, who is independent from the first and second lines of defense. Internal Audit regularly reviews both the first and second line to ensure that they are carrying out their tasks at the required level. The Board receives reports from audit, oversight and the business, and will act on any items of concern from any party; they will also ensure that the three lines of defense are operating effectively and according to best practice.

The interrelationship of the first and second lines of defense can be applied using the analogy of car crashes. For example, a group of teenagers is being told by a driving instructor the importance of wearing a seat belt while they drive to decrease the probability of death during a crash. You can have one group of teenagers who choose not to wear a seat belt, observe the speed limit, or follow traffic lights, etc. Similarly, you have another group of teenagers who choose to wear a seat belt, observe the speed limit, or comply with traffic light signals. For both groups, whether or not they wear the seat belt does not decrease the probability of whether or not they get into the crash. However, the number of deaths of people who get into car crashes is higher in the first group, because of their non-adherence to observing and following sound driving practices. In this analogy compliance is the driving instructor who is telling the group of teenagers the risk of not wearing a seat belt and the potential consequences if they were to get into an accident. The risks might include: getting ejected from the car or being thrown into a rapidly opening

frontal air bag; in both situations this could result in the individual being severely injured or dying. The teenagers are the first line defense ("risk owners") and the driving instructor is the second line of defense ("measures risk"). This is an especially important distinction because compliance does not tell the lines of business how to operate but makes them aware of the risks involved. It is up to lines of business to determine whether they are willing to take a risk or take a different course of action. Another important aspect that must be highlighted is that there is no such thing as no risk because banking in general is risky. The 1LOD has a responsibility to determine how much risk they are willing to take by establishing risk tolerance thresholds and compliance responsibility. In order for the 1LOD to establish risk tolerance thresholds, the 2LOD needs to build a risk control environment. Currently, the 1LOD for the Bank has some controls in place, however the control process is immature due to: 1) lack of continuous training and reinforcement, 2) lack of documented guidelines and procedures, 3) no established QA/second review process to monitor self-identified errors, 4) lack of 1LOD resources and knowledge of regulatory compliance, and 5) an immature operational risk management program. Lastly, FRBC needs to establish a compliance culture that has buy-in from executive management (this is addressed in Phase III – Establishment of CMS culture section).

IIIbi. Application of ERM Framework

At Trustmark, the FRBC has no authority over the operations risk management program. This program belongs to ERM, and ERM has a two-year plan to enhance the operational risk management program. In order to build a more 1LOD centric risk control environment, a working group will need to be put together that consists of a project manager, 1LOD senior management and stakeholders, and senior managers from FRBC and ERM. Since this is a 1LOD process, FRBC and ERM will function in an advisory-type capacity to provide risk and compliance insights. Also, they will be key stakeholders in the development of this process because the 1LOD controls are utilized to measure risk in the risk assessment and self-testing activities. Lastly, the working group will need to designate a point of contact on the 1LOD (i.e., senior manager) to ensure the group is meeting deadlines and deliverables are reviewed.

A proposed initiative from FRBC is to hire compliance officers and train them in the different areas of compliance and 1LOD operations. Then after two-years these individuals will be moved to the 1LOD as risk managers and they will function as coordinators with FRBC, Internal Audit, and for regulatory exams. The risk managers will be responsible for responding to compliance requests, internal audit exams, regulatory exams, and will develop and update 1LOD policies, procedures, and programs to ensure they are compliant with regulatory requirements. In addition, the risk managers will provide periodic ad hoc training to the

1LOD and communicate regulatory updates. This will ensure that the 1LOD is kept abreast of the changing regulatory environment. Currently, the Bank has BURCS who are the coordinators between 1LOD and FRBC. However, they lack the knowledge in regulatory compliance and the ability to function as risk managers.

Another process that FRBC has improved on is the consumer compliance risk assessments. The process collects control environment information. This information can be provided to ERM for the build out of their enterprise controls environment. In addition, this information can be used as a starting point for the working group to build upon. The working group will need to draft an action plan. The action plan needs to outline the strategies to build a risk control environment, resources assessment, and timeline for deliverables. The action plan will need to be presented to executive management and the Board for approval. Once approved, the working group will make adjustments to the action plan as needed and determine the criteria for pre/post implementation testing.

IIIc. Phase III – Establishment of CMS culture[4]

Compliance culture is a critical part of any organization's success, regardless of the organization's size, industry type, or business locations. Banks are no exception. Banks that prioritize executing viable compliance programs are better equipped to manage risk, protect their brand and reputation, and maintain trust with prospective and existing customers, board members, employees, and stakeholders.

A culture of compliance is a set of values, behaviors, and attitudes that guide employees to adhere to policies, procedures, and regulations. Everyone in the Bank must understand the importance of jurisdictional laws, industry regulations, internal policies, and general ethical values. Culture ultimately provides a foundation that shapes employees actions and decisions, which can make or break the long-term success of the Bank.

Non-compliance in the corporate culture can have significant reputational, legal, and financial costs for organizations. For example:

- Violation of laws can result in **fines and legal action, including imprisonment.**

[4] Whistleblower Security."6 Tips for Developing a Culture of Compliance.February 27, 2023. https://blog.whistleblowersecurity.com/blog/6-tips-for-developing-a-culture-of-compliance

- Compliance failure can also impact an organization's ability to conduct business. For instance, a company's breach of specific regulations may lead to **loss of licenses, suspensions, and reduced revenue.**
- Code of conduct and ethical scandals can **diminish customer, investor, and stakeholder trust.**
- Overall **reputation may tarnish**, leading to the downfall of an organization.

Creating a corporate culture that prioritizes high standards of behavior and ethics can be challenging. However, the cost of non-compliance could be detrimental to the Bank's future. Building a CMS program and culture Trustmark's size and complexity requires careful planning and consistent monitoring and review. The diagram below outlines the components of developing a compliance culture at the Bank and the following sections outline the details of each component.

1. Leadership: In order to establish an effective compliance culture there needs to be a top down approach in which executive and senior management set the tone, and it trickles down to employees. Their clear, enthusiastic commitment to compliance is essential. Leaders of the Bank should communicate the importance of compliance and hold themselves and those around them accountable. Leading by example is one of the best ways to perpetuate this culture. FRBC is currently working with executive management to propose an improvement plan of the compliance culture and will seek to obtain their buy in. FRBC will form a working group to determine the communication approach to the organization.

2. Action plan: Compliance initiatives cannot be executed without clearly outlined action plans. Policies and procedures should be straightforward, concise, and communicated consistently by FRBC. For example, frequent email communications or verbal discussions about expectations should be a priority for the Bank. FRBC is currently developing a dedicated compliance site that provides: 1) an inventory of FRBC policies,

programs, and procedures, 2) points of contact for subject matters experts in the different areas of compliance, and 3) a FRBC newsletter that communicates emerging regulatory risks.

3. Training: Compliance training needs to be engaging, interactive, and tailored to the Bank and interdepartmental needs to help employees understand the importance of compliance. Education should be ongoing, repeated periodically, and updated to align with new laws, regulations, and industry best practices. FRBC is currently utilizing an out-of-the box solution from a vendor who develops and updates compliance training. The training has received a lot of criticism from the organization due to the large number of training modules assigned to associates. A gap analysis was conducted on training and a number of inefficiencies were identified:

- The large number of assigned training courses is due to the inability to aggregate courses. For example: instead of having training for each regulation the regulations can be aggregated into one training course (i.e., all credit regulations can be rolled into a Credit Compliance training).
- Limited ability to customize training – the vendor training is not updated frequently and in order to make changes there is dependency on one dedicated resource who is responsible for the whole organization.
- Inability to develop/administer courses in-house. The Bank is highly dependent on the vendor.
- There are a large number of employees who are incorrectly assigned training due to issues with the assignment of job families.
- Lack of executive management support related to communicating and enforcing the importance of compliance training.

A project plan is being put together which will take one year to complete. The objectives of the project plan are to:

1) Identify a different vendor or renegotiate the existing contract in order to have the ability to customize the training modules
2) Have the ability to utilize customization with current resources or aggregate vendor courses
3) Evaluate the current system of assignment using job families and identify an approach to better assign compliance training
4) Establish a communication piece to emphasize the importance of the training and gain executive support
5) In the long term, the Bank will develop and administer course content in-house to eliminate vendor dependency

4. Prioritize continuous improvement: This is similar to the expectation of employees to strive for continuous improvement, it is essential that the Bank looks internally to assess areas to change and grow. The CMS program should not be static and must be regularly reviewed and updated to remain practical and relevant. Maintaining a dynamic compliance program includes:

- Keeping up to date with changes in regulations and industry standards
- Being open to feedback from employees and other relevant stakeholders

FRBC is currently improving training by: communicating on a weekly basis to senior management and the lines of business any important regulatory changes. FRBC staff are required to take 40 hours of external training to keep updated on emerging regulatory risks and the regulatory environment. Additionally, management has been encouraging FRBC staff to obtain professional certifications in their respective compliance areas (i.e., Certified Regulatory Compliance Manager, Fair Lending Expert, etc.). FRBC has committed to the regulators that 40% of FRBC associates will obtain a compliance certification by the end of 2024. Lastly, as mentioned previously FRBC is creating a dedicated compliance site. The site will include a feedback link for the organization to allow for non-FRBC associates to provide feedback to Compliance. This information will provide potential enhancement opportunities to better communication opportunities within the organization.

5. Speak-up culture: A key part of compliance is allowing employees to feel comfortable raising issues and reporting violations without fearing retaliation. This means creating a culture that encourages open and transparent communication and providing the means for employees to voice their concerns. One example is having an ethics helpline, which allows people to report anonymously. The Bank has a dedicated Ethics hotline that provides employees the option to anonymously report unethical behavior to the organization. The hotline is managed by a vendor to protect the confidentiality of the process. In addition, employees are provided resources to submit whistleblower complaints which work similarly to the Ethics hotline.

6. Use tools that prove commitment to compliance: As mentioned above, failure to have sound plans and processes for an organization's compliance program can lead to its downfall. One way to reduce this possibility is to invest in tools that allow the FRBC to monitor concerns and organize workflow for risk management. Compliance case management systems enable sophisticated ways to stay on top of the corporate culture. With technological advancements and businesses growing their operations across the globe, the Bank's tools must also expand to keep up with all the moving parts. Using these resources shows the Bank's commitment to policies and procedures and demonstrates that compliance is taken seriously.

FRBC has a dedicated resource who identify technology and vendor improvements for the CMS program. The Strategic Initiatives Manager is currently working on identifying vendor solutions to automate many of the manual processes being put in place. One example includes the dedicated compliance site, instead of receiving inquiries from the lines of business via email, these inquiries will be submitted through the compliance site. This will ensure that inquiries are being directed to the right compliance associate and responded to in a timely manner.

In order to measure the effectiveness of the compliance culture the following factors will be taken into consideration:

- Tracking of compliance training completion
- Reviewing the number and magnitude of compliance incidents and violations
- Conducting interviews with 1LOD management
- Running focus groups or surveys to gather feedback on employee perception of the corporate culture
- Using independent auditors to assess the Bank's compliance policies

These are metrics that the Bank will use to understand the effectiveness of their code of conduct and other internal policies and make improvements where needed.

IIId. Phase IV – Expansion of CMS staff, technology, and process

This will be one of final phases of the action plan. In this phase of the project, the Director of FRBC will need to conduct a staffing and technology plan that is comprised of a multi-faceted approach that addresses departmental needs for technology, skill sets, education, experience, professional development as well as, understanding the number of associates that are necessary to complete mission critical tasks. It will also consider the existing staff competency and developmental needs and future associates to formulate a sustainable CMS program. Lastly, the plan will determine whether new processes need to be developed or if existing processes can be enhanced as a result of this plan. The program contemplates every compliance function necessary for a complete program that meets the obligations for fulsome oversight of consumer compliance activities. Given that each function may require a unique set of skills to operate effectively, the FRBC is organized into sub-groups that are specialized. These groups are led by managers who are experienced in that group's subject matter and includes Consumer Compliance Testing and Monitoring, MQC Testing and Monitoring, Fair Lending Analytics, Home Mortgage Disclosure Act ("HMDA")/CRA Regulatory Reporting, CRA Monitoring and Reporting, General Compliance Risk Assessment (GCRA), FRB Risk Assessments, Fair Banking Management, Strategic Initiatives - Regulatory

Change/ Complaint Oversight/Exam Management. As noted above there are processes noted above that are being improved which include: vendor management, change management, compliant management, and the compliance governance and oversight process. The enhancements of existing processes and development of new processes will bring about a potential need for additional resources which include staff and technology. Therefore, it would be important that a resource assessment be conducted to understand the need. The following lists the actions that would need to be taken to develop a documented process for assessment.

Staffing Assessment

1. Develop a staffing assessment methodology document which outlines the methods of assessment, frequency of assessment, and alternatives for staffing should that be required.
2. Enhance the information data collection of each associate's compliance experience, professional credentials, education, relevant training, and current development plans.
3. Enhance the skill set assessment to include: the level of technical knowledge by regulation, the most recent performance evaluation results, an assessment of the individual's ability to be perform other roles within FRBC, and the Director's assessment of each associate.
4. Enhance the assessment with time studies by task and function.
5. Enhance the assessment to include all associates within FRBC to 1) provide consistency and 2) to understand crossover skills that may be used within the department.
6. Consider the requisite training and experience needed to fill the various positions within the department and adjusted job descriptions accordingly.
7. Consider staff turnover in prior year and the impact to achieving compliance initiatives on a short- and long-term basis.
8. Consider staff retention options and succession planning.
9. Evaluate current vendors and tools being utilized by FRBC and identify opportunities to automate manual processes, and improve existing processes

Each functional group was assessed separately[5] to determine both the competency and ability to complete the anticipated workload within established timelines. Separate documentation outlining the skills, knowledge, education, certifications, performance evaluation of associates and the supporting methodology are considered a part of this assessment.

Technology Assessment[6]

1. Discovery phase – The purpose of the discovery phase is to deeply understand the current state, the problem, and the reason for the problem/objective. The following outlines the steps for this phase.

    a. Understanding the current technology eco-system – This includes both the solutions currently being used as well as the systems and processes used to connect those systems (i.e., looking through the lens of a business process, and looking at what data is moved along the way).

    b. Understanding the problem – This is defined as the end-user experience.

    c. Understanding the user experience – This is defined as the current issues that FRBC is struggling with and the ability to link the issues back to the problem.

2. Analysis – At the end of the discovery phase, there is enough information to understand the end goal and how to get there (i.e., action plan). In this next step, the user will analyze the tools and solutions that are currently being utilized at a granular level. This will provide insight on whether the tools and solutions are being fully utilized, underutilized, being misused, or no longer meeting the needs of the department. The objective of the analysis is to identify the gaps and weaknesses of the tools and solutions currently being used. Also, this analysis will identify the technology requirements for the department.

3. Define and Develop – At this point, the goal has been defined, there is an understanding of the problem and environment, and the identification of gaps and weaknesses. At this phase, the technology vision will be developed and defined though the lens of FRBC operational requirements.

[5] Assessment occurred in Q1 2022 and will be conducted again in Q4 2023.
[6] Engineess.How to Conduct a Technology Assessment: A Four-Step Guide.August 12, 2021. https://www.enginess.io/insights/how-to-conduct-technology-assessment?l=en-us

4. Document – The final step is to develop a well-documented plan. The final document will include:
    a. A high-level overview
    b. A detailed explanation of the objective(s) or problem that will be solved
    c. Details of implementation and deployment
    d. Details of project timelines and ownership

Once the staffing and technology assessments have been completed the results of the assessment need to be communicated to senior management and executives to gain buy-in to obtain additional resources. There was a staffing assessment conducted in 2023 due to the departure of the Director of Enterprise Risk and Compliance in August 2023. The former director was over ERM and Compliance. The Chief Risk Officer eliminated this position and separated ERM and Compliance into two different departments. The Director of FRBC was put over Compliance. This resulted in the following organizational changes:

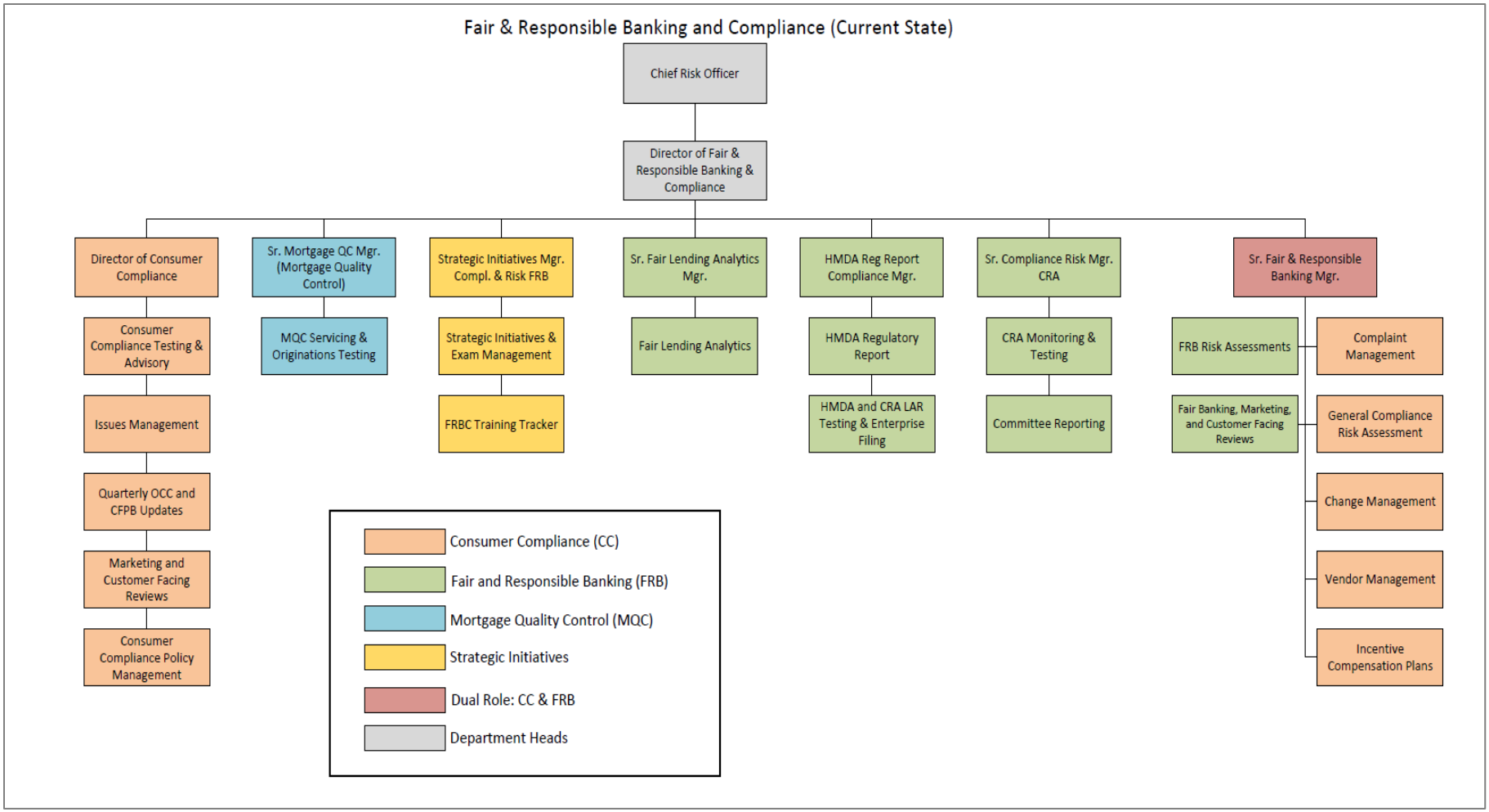
- Consolidated compliance functions within Enterprise Risk Management (ERM) to the FRBC Group (consumer compliance, risk assessments, complaint monitoring, and consumer regulatory management)
- Consolidated the consumer compliance and Fair and Responsible Banking (FRB) functions reporting line under the Director of FRBC
- Added leadership positions for Consumer Compliance, MQC, and Fair and Responsible Banking ("FRB"). (Consumer Compliance Director, Sr. Mortgage Quality Control Manager, and Sr. FRB Manager)

As a results of the organization change, additional resources were identified using the methodology mentioned above and additional five employees were needed. However, the strategic plan that has been laid out will result in the need for additional resources to operate the additional processes that will be managed by FRBC.

IIIe. Phase V – Implementation of Compliance Risk Management Structure

The current CMS program has four pillars which include: consumer compliance and testing, MQC, FRB, and Strategic Initiatives. The consumer compliance and testing group provides monitoring and testing for credit compliance, privacy compliance, and deposit compliance. The monitoring and testing of FRB compliance is handled by the FRB group. MQC group conducts quality assurance testing for the Enterprise Mortgage group. In order to maintain their level of independence the MQC group reports directly to FRBC. The Strategics Initiative group is headed by the Strategic Initiatives Manager, which is a newly created position in 2022 and is focused on developing standardized procedures for exam management as well as

coordinating exams within FRBC. In addition, the position is charged with identifying solutions and tools that FRBC and ERM can utilize for monitoring, testing, and reporting. As mentioned previously, the Strategic Initiatives Manager is currently working on developing a dedicated compliance site. The diagram below illustrates the current organization structure.


Fair & Responsible Banking and Compliance (Current State)
Chief Risk Officer
Director of Fair & Responsible Banking & Compliance
Director of Consumer Compliance
Consumer Compliance Testing & Advisory
Issues Management
Quarterly OCC and CFPB Updates
Marketing and Customer Facing Reviews
Consumer Compliance Policy Management
Sr. Mortgage QC Mgr. (Mortgage Quality Control)
MQC Servicing & Originations Testing
Strategic Initiatives Mgr. Compl. & Risk FRB
Strategic Initiatives & Exam Management
FRBC Training Tracker
Sr. Fair Lending Analytics Mgr.
Fair Lending Analytics
HMDA Reg Report Compliance Mgr.
HMDA Regulatory Report
HMDA and CRA LAR Testing & Enterprise Filing
Sr. Compliance Risk Mgr. CRA
CRA Monitoring & Testing
Committee Reporting
Sr. Fair & Responsible Banking Mgr.
FRB Risk Assessments
Fair Banking, Marketing, and Customer Facing Reviews
Complaint Management
General Compliance Risk Assessment
Change Management
Vendor Management
Incentive Compensation Plans
Consumer Compliance (CC)
Fair and Responsible Banking (FRB)
Mortgage Quality Control (MQC)
Strategic Initiatives
Dual Role: CC & FRB
Department Heads

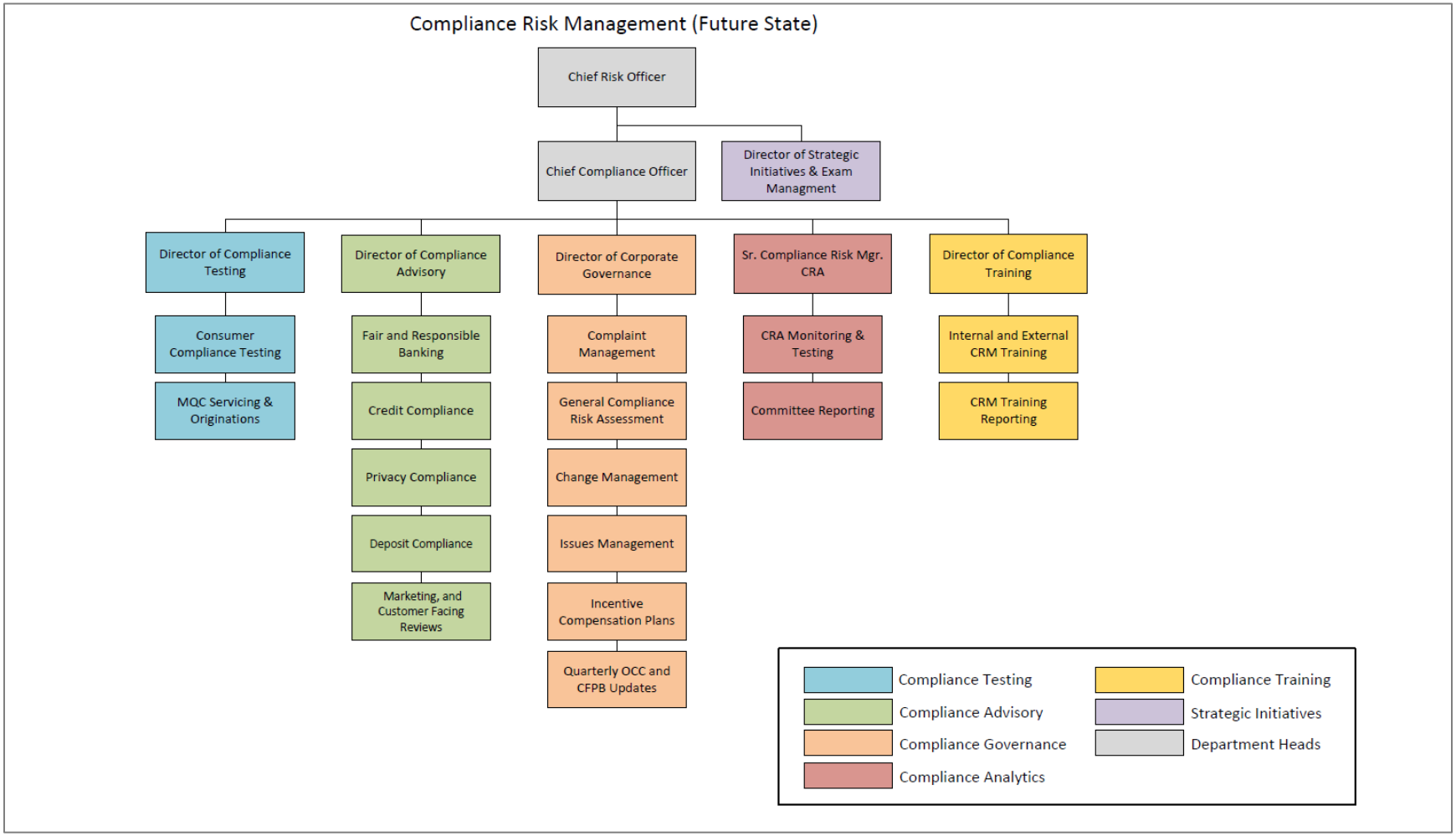
In the current state, there was an emphasis to grow the FRBC group to address a regulatory issues and demonstrate to the regulators the Bank's commitment to being FRBC compliant with the Office of the Comptroller of the Currency ("OCC") requirements. The issue has been resolved with the Bank wanting to offer new products and services and expand to new markets. A couple examples include: The opening of a loan production office Atlanta, Georgia in 2022 which is a new market for the bank and the implementation of a special credit program for underserve communities in the Bank's footprint.

Although there were already a number of reorganization changes to the CMS program, the program still has to evolve to keep up with the regulatory requirements for a mid-size level bank. There are some nuisances with the current state that were mentioned earlier. The compliance testing and advisory function are contradictory functions. The Compliance testing objective is to independently assess 1LOD and 2LOD risk. The group that is providing the testing function cannot provide advisory advice to 1LOD and 2LOD especially since the advisory function is part of the overall testing. Secondly, there is one person who is well versed in deposit, privacy, and credit regulations. There should be multiple individuals trained or there should be designated subject matter experts in these respective areas. Thirdly, the MQC is an independent testing group for Mortgage, however they function similarly to Compliance Testing. In order to gain efficiency these two groups should be combined into one testing group.

A couple of other gaps that need to be addressed are: heavy reliance on vendor solutions and the need for more robust analytics and automation. FRBC can benefit from having a dedicated analytics group that can provide centralized reporting, analytics, and automation for manual processes. Secondly, the reliance on vendor models makes it difficult for customization. For example, the CMS program is currently utilizing a vendor to execute Compliance training for the organization. The vendor is not updating the training modules to include regulatory changes. FRBC could consider developing Compliance training internally to ensure that training remains current.

The Strategic Initiatives group lacks the proper authority to coordinate exam management activities across the organization. Furthermore, the group is not only being utilized by FRBC but ERM as well. Due to the nature of the Strategic Initiatives group, the group should report directly to the Chief Risk Officer. Additionally, the CMS program needs to be expanded to have the following five pillars: analytics, advisory, independent

testing, training, and corporate governance. This structure will be able to support the increasing regulatory demands as the Bank continues to grow. The following diagram illustrates the proposed CMS program structure in the future state.



The following outlines the details of each pillar.

1. Compliance Testing – This group will provide independent testing of 1LOD and 2LOD. There will be senior managers who specialize in MQC, FRB, credit, privacy, and deposit compliance. These senior managers will report directly to the Director of Compliance Testing.
2. Compliance Advisory – This group will consist of subject matter experts in FRB, credit, privacy, and deposit compliance. There will be senior managers for each of these areas and they will report to the Director of Compliance Advisory. Each area will respond to 1LOD inquiries approvals, review and update 1LOD procedures, update 2LOD policies, programs, and procedures, conduct self-testing and monitoring, and participate in internal/external exams.
3. Corporate Governance – This group will be comprised of senior managers who are over the complaint management, GCRA, change management (vendor management and regulatory intelligence), issues management, incentive compensation plans, and quarterly OCC and CFPB updates. The senior managers will report directly to the Director of Corporate Governance.
4. Compliance Analytics – Due to the increasing demands of Big Data and the need for analytics to support business decisions, a dedicated group of analysts is warranted. This group will consist of data scientists who will report directly to the Director of Compliance Analytics. The associates in this group specialize in technology, statistics, modeling, and analytics and will fill a skill gap lacking in the current CMS program. This specialized group will be responsible for automation, reporting, data validation, analytics, and statistical modeling for all of compliance. The advantage of having this group is the data being utilized for reporting and business decisions will be highly accurate and this group will create efficiencies by eliminating manual processes.
5. Compliance Training – This group will develop and update Compliance training across the organization. There will be associates who specialized in compliance training and report to the Director of Compliance Training. This group will partner with the Talent Management group to ensure that update training is being provided to all employees and provide regular reporting. In addition, this group will be responsible for providing training reports for committee meetings, Board reporting, and internal and external exams.

As mentioned above, the Strategics Initiative group will be moved under the Chief Risk Officer and the senior manager will be the Director of Strategic Initiatives and Exam Management.

The new CMS program structure is aligned to that of other mid-size level banks in the industry. Furthermore, it addresses the deficiencies of separating the roles of independent testing and advisory. There is better compliance coverage by having multiple people in the advisory capacity instead of relying on one person. The independent testing for compliance and MQC are combined into one group to create efficiency. The structure also addressing gaps with analytics, reporting, and training. Also, there will be dedicated resources to ensure the continued growth and enhancements to the GCRA, complaint management, issues management, and vendor management. Lastly, the restructuring will warrant the department name to be changed from FRBC to Compliance Risk Management. This naming convention better represents the restructured CMS program and aligns to the naming convention being utilized by other mid-size level banks.

IV. Financial Impact

IVa. Investment Size and Type

In general terms, compliance is costly to all banking organizations. Compliance cost refers to all expenses incurred for a bank to comply with industry regulations and the ongoing cost for remaining compliant with legal and regulatory rules. The cost of compliance will increase as the regulation standards in the banking industry change and intensify, and as the Bank continues to expand its Company's footprint into neighboring states. There are other costs that need to be taken into consideration, which are regulatory risk and conduct costs. Regulatory risk is the risk the Bank faces due to potential changes in the rules going forward (what is also referred to as "emerging risks"), and conduct costs, which are the regulatory fines the Bank incurs for non-compliance to the regulations. The primary focus for this project will be on compliance cost because the objective of the project is to restructure the current CMS program for long-term sustainability and to adapt to the growth of the Bank. The regulatory risks and conduct costs will be briefly discussed to gain an understanding of the potential risk should the Bank decide not to make any changes to the current CMS program.

The main compliance cost drivers of this proposal include the need for additional personnel, certifications and ongoing training for existing staff, investment in technology, and a roadmap. It should be noted that the 1LOD's time is not taken into account for the development of the risk controls environment. Since they are risk owners, the 1LOD will need to form a working group and FRBC will participate in a consulting compacity advising from a regulatory perspective. The working group needs to provide an action plan. Lastly, once the restructuring of the CMS program has occurred there are ongoing costs related to sustainability and the continued re-evaluation of resources to ensure there is adequate compliance coverage. This is not something that will be taken into account for this proposal but something that is worth mentioning.

IVb. Regulatory Risk and Conduct Costs

A brief discussion of the regulatory risk and conduct costs is important to note; should the Bank decide not to proceed with this proposal. As mentioned in the prior sections, the current CMS program was built specifically for a community/small bank and has gone through significant changes since 2016 to be able to withstand regulatory scrutiny. However, the current CMS program is not sustainable in the long-term as the Bank continues to grow. There are sustainability risks that come with not continuing to evolve the CMS program and other risks such as the Bank not remaining compliant with current rules and regulations. A

question that comes up in executive and Board meetings is, "*So what, if we violated all these rules, what's the penalty, what's it going to cost our bank?*"[7]

The Financial Institution Reform Recovery and Enforcement Act ("FIRREA") provisions were written to address violations of banking laws or regulations, and state that FIRREA penalties including civil money penalties can be assessed for non-compliance. FIRREA gives all compliance rules and regulations a penalty provision for ***any*** violation. Also, this gives regulators the ability to assess a fine against banks for any violation identified in the course of their examinations of banks. There are three tiers and levels of penalties, and the amount of money that can be assessed as a penalty corresponds to the seriousness of the violation. The following outlines each of these tiers[8]:

- Tier I – The penalty is approximately $7,500 per violation; per day the violation is outstanding. For example: A bank would have a Truth in Lending Act ("Reg Z") issue if it did not issue a loan estimate until the fifth day and Reg Z requires the estimate to be provided by the third day. The bank would have violated Reg Z for two days which amounts to a $15,000 violation (i.e., $7,500/day X two). In addition, each regulator has the ability to set its own FIRREA civil money penalty tier amount. In this case a regulator can increase the penalty from $7,500 to $8,300; the penalty amounts are published in the Federal Register every year and indexed to inflation.
- Tier II – The penalty is approximately $37,500 per violation; per day if it is a reckless situation, meaning the bank should have known that this was happening and chose not to fix it or do anything about it. A penalty can also be assessed if there is a pattern of misconduct that causes more than a minimal loss to the bank (i.e., financial loss). This tier addresses material impact to the bank's liquidity or bottom line.
- Tier III – The penalty is approximately $1.5 million dollars per violation; per day if that violation is committed knowingly, or recklessly causing substantial loss to the bank.

The following provides is a recent example of Bank of America's consent order and the consequences for having an ineffective CMS program.

[7] American Banker Association.Certified Regulatory Compliance Manager Online Prep Course.FIRREA Civil Money Penalities

[8] American Banker Association.Certified Regulatory Compliance Manager Online Prep Course.FIRREA Civil Money Penalities

Bank of America Consent Order

The consent order that required Bank of America to compensate consumers who were charged unlawful non-sufficient fund fees if they had not yet been refunded. Bank of America harmed customers by double-dipping on fees, withholding credit card rewards and opening fake accounts. The bank was hit with penalty fees by the Office of the Comptroller of the Currency ("OCC") and the Consumer Financial Protection Bureau ("CFPB").

In the CFPB article entitled, "*CFPB Takes Action Against Bank of America for Illegally Charging Junk Fees, Without Credit Card Rewards, and Opening Fake Accounts*," it stated[9]:

"Today, the Consumer Financial Protection Bureau (CFPB) ordered Bank of America to pay more than $100 million to customers for systematically double-dipping on fees imposed on customers with insufficient funds in their account, withholding reward bonuses explicitly promised to credit card customers, and misappropriating sensitive personal information to open accounts without customer knowledge or authorization. The Office of the Comptroller of the Currency (OCC) also found that the bank's double-dipping on fees was illegal. Bank of America will pay a total of $90 million in penalties to the CFPB and $60 million in penalties to the OCC.

Bank of America wrongfully withheld credit card rewards, double-dipped on fees, and opened accounts without consent," said CFPB Director Rohit Chopra. "These practices are illegal and undermine customer trust. The CFPB will be putting an end to these practices across the banking system."

In total, Bank of America had to pay $250 million to consumers and for regulatory penalties. This amount does not include the compliance cost needed to improve 1LOD and 2LOD controls & oversight and enhancements & sustainability to the CMS program to ensure the Bank of America is complying with laws and regulations.

There are two areas that Bank of America was cited for: representment fees and credit card practices. Representment is the practice of declining a transaction due to insufficient funds and charging a non-sufficient funds ("NSF") fee, then the bank pays the transaction and charges the customer a second overdraft fee. This practice did not end until February 2022 and is considered an unfair act or practice under UDAAP. Also, the practice of charging either an NSF or an overdraft fee on re-presented

[9] CFPB. CFPB Takes Action Against Bank of America for Illegally Charging Junk Fees, Without Credit Card Rewards, and Opening Fake Accounts.July 11, 2023

transactions was considered unfair and deceptive. Lastly, deposit agreements, disclosures, and schedule of fees contained materially misleading representation and omissions regarding representment fees[10]. This was activity that should have been identified in Bank of America's UDAAP program if they were conducting periodic self-testing on deposit fees, however it was left unchecked and the practice of representment was not discontinued until early 2022.

In regard to Bank of America's credit card practices, the Bank engaged in deceptive acts or practices in violation of Consumer Financial Protection Act ("CFPA") in connection with promotions of rewards credit cards. It also finds that the Bank violated the Truth in Lending Act ("TILA") and the Fair Credit Reporting Act ("FCRA") in connection with certain practices relating to the opening of credit card accounts. The Bank had online advertisements that did not expressly state that bonus offers were limited to online applications and gave a false impression that offers were available to all applicants regardless of the application channel used. There were also some consumers targeted to apply for a rewards credit card, who did apply, and did not receive the promised advertised bones because Bank's employees did not accurately complete the application process. With regards to credit opening practices, Bank employees sometimes submitted applications for and issued credit cards without consumers' consent. In addition, Bank of America used or obtained consumer reporting in connection with these applications. The employees were enticed to do this because of Bank of America's management established sales goals[11]. The root causes of Bank of America's failures are: inadequate UDAAP testing program, sales practices, inadequate 1LOD/2LOD marketing review process, 1LOD and 2LOD control failures related to Truth in Lending Act and Fair Credit Reporting Act.

These violations could have been prevented if Bank of America were proactive and conducted periodic checks on their CMS program to identify deficiencies in their program and made the appropriate enhancements/adjustments. This is a perfect example of what happens when a bank does not evolve their CMS program and when the 1LOD does not have an established risk control environments. Bank of America is an example of when an organization does not continue to evolve their compliance program

[10] Ballard Spahr. Culhane, John. L. Larson. Kristne E.*" CFPB and OCC announce consent orders with Bank of America involving deposit account representment fees and credit cards.."* July 12, 2023

[11] Ballard Spahr. Culhane, John. L. Larson. Kristne E.*"CFPB and OCC announce consent orders with Bank of America involving deposit account representment fees and credit cards.".* July 12, 2023

and the costs for non-compliance. This is something that the Bank's management should take into consideration while evaluating this proposal.

IVc. Compliance Cost Drivers Estimates

The following provides the annual estimated cost for adding personnel, onboarding new technology, the cost to provide training and certification costs for existing FRBC staff, and the proposed roadmap

Personnel

The time task study considers the minimum and maximum hours that are needed to complete the essential elements of compliance assignments. It recognizes that tasks may take differing periods based on an associate's familiarity with Trustmark practices, knowledge/skill set, and level of experience. The aforementioned factions within each team vary from individual to individual and these differences are accounted for by selecting the average time to base the necessary FTE count to fulfill accountability for meeting deadlines and accurate completion of work.

When the FTE count is more or less than the current staffing levels, consideration may be given to redistributing workload, adjusting schedules in accordance with risk principles, and/or evaluating different technology to further automate and/or streamline workflow processes.

FTE Conclusion

The following tables outline the changes to the total number of employee pre- and post-restructuring.

Function (Pre-Restructuring)	Total
Consumer Compliance Testing & Advisory	9
MQC Servicing and Originations	7
Strategic Initiatives & Exam Management*	2
Senior FRB Manager	1
Complaint Management and Change Management	1
GCRA	2
FRB Risk Assessment	2
Fair Banking	2
Fair Lending Analytics	4
HMDA Regulatory Reporting	6
CRA	8
Total	**44**

Team will be moved under Chief Risk Officer

Function (Post-Restructuring)	Total
Director of Compliance Testing	1
Consumer Compliance Testing	7
MQC Servicing & Originations	7
Director of Compliance Advisory	1
Fair and Responsible Banking	23
Credit Compliance	3
Privacy Compliance	3
Deposit Compliance	3
Director of Corporate Governance	1
Complaint Management & Change Management	2
GCRA	2
Issues Management	2
Vendor Management	2
Director of Compliance Analytics	1
CRM Reporting	2
Data Validation, Analytics, Models, and Dashboards	2
Director of Compliance Training	1
Internal and External Training	1
CRM Training Reporting	1
Total	65

Net change	**21**

Recommendations Based on the Time/Task Analysis

In the new staffing model, there will be an increase of 21 compliance personnel. The following outlines the details of the additional full time employees (FTE).

Compliance Testing: The Director of Compliance Testing will be added to the new staffing model. This position will provide governance and oversight over Consumer Compliance/MQC monitoring and testing program. The lower level managers and analysts in the Consumer Compliance Testing & Advisory and MQC Servicing and Originations from the old staffing model will be moved under the Director of Compliance Testing. Additionally, the two senior managers for consumer compliance and MQC will report directly to the new director. This new staffing structure will allow for the compliance testing group to be an independent testing function for 1LOD and compliance.

Compliance Advisory: The Director of Compliance Advisory, four senior managers, and one FTE for Fair Banking will be added to the new staffing model. These positions will provide the compliance advisory in FRB (i.e., Fair Lending, Fair Banking, HMDA, and CRA), credit, privacy, and deposit. FRBC in the old staffing model will be moved under the Director of Compliance Advisory. Credit compliance, privacy compliance, and deposit compliance will be newly created groups to provide better coverage in these areas and reduce the risk of only having one subject matter expert (SME) in these areas. The senior managers in these areas will report to the new director. These groups will provide compliance oversight and governance of the 1LOD.

Corporate Governance: The former Director of Consumer Compliance will be moved to manage the Corporate Governance team and the title will be changed to Director of Corporate Governance. Three senior managers and two FTEs will be added to the staffing model. The complaint management & change management, GCRA, and vendor management teams will be moved under the Director of Consumer Compliance. Issues management was managed by the former Director of Consumer Compliance, the additional FTEs (a senior manager and analyst) for this process are included in the added headcount. This newly created structure will provide for better oversight for these functions and the senior managers in these areas will report to the new director.

Compliance Analytics: The Compliance Risk Manager who is conducting analytics for the FRB risk assessments will be promoted to the Director of Compliance Analytics. Two senior managers and two FTEs will be added to the staffing model. Both senior managers will report to the new director. This group will consist of data scientists who will provide reporting, data, analytics, and dashboards for Compliance Risk

Management. The group will serve as the centralized group for these functions and bring consistency to compliance reporting and provide efficiencies to the department.

Compliance Training: The Director of Training and two FTEs will be added to the staffing model. This group will be responsible for tracking compliance training across the Enterprise and within Compliance Risk Management. Also, they will assist in the development and enhancement of compliance training across the enterprise. Lastly, they will be responsible for creating and validating training reports for committee meetings, Board reporting, and internal and external exams.

The following provides the total estimated cost of the 21 additional FTE, please note that an average salary was used to determine the total cost. The total estimated cost is approximately$2.5 million (rounded up).

Position Type	Total	Average Salary	Total Salary
Director	4	$170,000	$680,000
Senior Manager	9	$130,000	$1,170,000
Compliance Officer	8	$80,000	$640,000
		Total Cost	**$2,490,000**

Technology

The restructuring of the CMS program will result in the need to replace existing technology and onboard new technology to meet the needs of the department. The department needs to replace the current complaint management and compliance training software. The current technology is outdated and not robust enough to meet the growing needs of these processes. As mentioned in the *'Strategy and Implementation'* section the 1LOD and FRBC needs to make improvements to the complaint management process. The current system is not user friendly; users have difficulty with inputting complaints and the system has limited customization options and reporting. Lastly, the system does not have sophisticated algorithms to categorize complaints by compliance regulations and conduct 1LOD and FRBC QA/QC work on complaint responses.

Currently, compliance training is being provided by a vendor solution who provides out of the box training modules. FRBC selects the modules that they want to deploy to the organization. The training modules have limited customization options and are not updated frequently to keep up with regulatory changes. Additionally, the reporting capabilities in the current system are extremely limited. A combination of a new software solution and the ability to develop inhouse training will help to address these issues.

In regard to new software, there is need for the department to have a dedicated CMS software. In the long term the software will save on operational costs. The CMS software can automate compliance monitoring and eliminate the need for investing in more personnel and resources. Additionally, the software can proactively track regulatory changes and flag risks that need to be evaluated by the department.

With the creation of the dedicated analytics team tools need to be provided to streamline the department's data, analytics, and reporting. There is a need for the department to have a dedicated data mart. The data mart will be the central repository of compliance data. The benefits of having a data mart includes improvement to end-user response time by allowing users to have access to specific data they need, a condensed and more focused version of a data warehouse, and customizable data. Lastly, tools for cloud computing platform, geocoding, and thermal mapping are needed to support existing functions. The following table outlines the estimated annual cost for the technology needed for the proposed restructuring. The total estimated cost is approximately $1.36 million (rounded up).

Application	Monthly Cost	Total # of Users	Annual Cost
Replacement Software			
Complaint Management Software	$3,000	150	$450,000
Compliance Training Software	$3,000	70	$210,000
New Software			
Compliance Management System	$1,500	150	$225,000
PowerBI Datamart	$5,000	70	$350,000
Geocodio	$2,500	30	$75,000
ArcGIS	$1,000	15	$15,000
Azure	$1,000	30	$30,000
		Total Annual Cost	**$1,355,000**

Certification/Ongoing Training

Regulatory knowledge and staying abreast of emerging compliance risk is essential to the sustainability of an effective CMS program. It is important that the existing staff obtains compliance certifications because it increases associates' knowledge, enhances career and professional development, and it increases staff credibility as a compliance professionals within the banking industry and with regulators. The most recognized certification in the compliance industry is American Bankers Association ("ABA") Certified Regulatory Compliance Manager ("CRCM") certification. This certification demonstrates expertise in the regulatory compliance field. There are other compliance certifications that are universally recognized in the compliance industry which include the: Fair Lending Expert, Certified Mortgage Compliance

Professional, Community Reinvestment Act Certified Professional, Certified Anti-Money Laundering Specialist, and Certified Internal Auditor certifications, to name a few. These certifications demonstrate expertise in specific area(s) of compliance. These certifications require individuals to pass a formal exam and upon completion, there is a requirement for continuous training in order to maintain the certification.

The FRBC team currently maintains 16 professional certifications which adequately support the need for specialized expertise across the team. There is one additional certification that is on track for completion in 2023. Expectations are that associate career development will continue through certifications, participation in conferences and American Bankers Association working groups, and/or external compliance training delivered through regulatory agencies and industry compliance training providers. The table below provides the estimated cost of certification and ongoing training for FRBC associates who have or are in the process of obtaining a certification. Additionally, the table provides the estimated cost of associates who are recommended to obtain certification in their respective areas. The total cost for new employees to obtain a certification is $80,942 and the ongoing annual training cost is $32,059, for a total overall training cost of $113,001.00. The details are provided below:

Ongoing Training and Annual Certification Fees

Certification	Existing Employees	Annual Renewal	Ongoing Training	Total Cost
Certified Regulatory Compliance Manager (CRCM)	9	$299	$350	$5,841
Fair Lending Expert	6	$295	$350	$3,870
Certified Mortgage Compliance Professional	0	$100	$350	$0
Community Reinvestment Act Certified Professional Certification (CRACP)	1	$395	$350	$745
Certified Internal Auditor	1	$120	$350	$470
Total Annual Cost for Existing Employees	**17**	**$1,209**	**$1,750**	**$10,926**

Certification	New Employees**	Annual Renewal	Ongoing Training	Total Cost
Fair Lending Expert	2	$299	$350	$1,298
Certified Regulatory Compliance Manager (CRCM)*	13	$295	$350	$8,385
Certified Mortgage Compliance Professional	8	$100	$350	$3,600
Community Reinvestment Act Certified Professional Certification (CRACP)	2	$395	$350	$1,490
Certified Internal Auditor	8	$120	$350	$3,760
Certifications/Training for Analytics Team	4	$300	$350	$2,600
Total Annual Cost for New Employees	**37**	**$1,509**	**$2,100**	**$21,133**

Total Annual Cost for Ongoing Training	**$32,059**

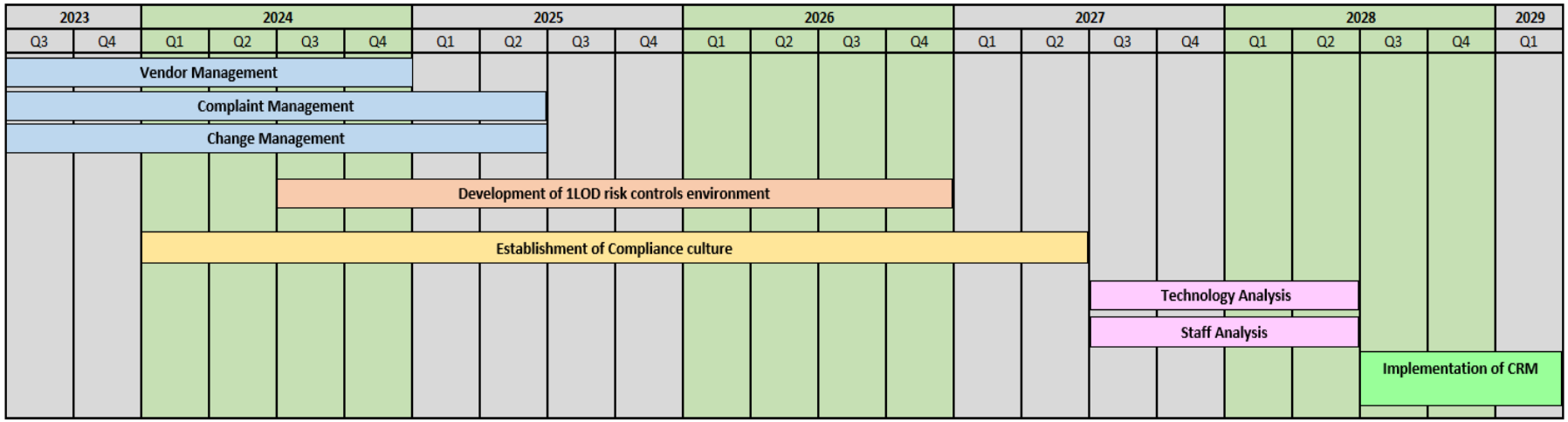
Total Overall Training Cost	**$113,001.00**

CMS Restructuring Roadmap

Legend	
Phase I	Improvement of current CMS program
Phase II	Development of 1LOD risk controls environment
Phase III	Establishment of CMS culture
Phase IV	Expansion of CMS staff, technology, & process
Phase V	Implementation of CRM Structure

The Bank's overall culture when it comes to significant change is slow and in response to issues identified, management takes a more reactive approach. Therefore, the timeframe to implement this type of approach needs to be strategic and methodical to take into account the culture and to gain buy in from 1LOD, senior and executive management. Therefore, a four year roadmap is being proposed to execute the five different phases and is provided below. This will not be an added expense to the Bank, since the participants are already employees of the Bank. However, the initiatives in this proposal will create a need for employees to assume added responsibilities. Also, there is some overlap between the phases because there are phases that do not need to be completed in order to start the next phase.

For example: Phase I is improvement to existing FRBC processes and 1LOD is managing Phase II. FRBC can continue to work on addressing the deficiencies and still work in a consulting compacity for 1LOD. The restructuring itself will require executive and Board approval and the proposed plan will be modified to best suite the needs of the organization.



IVd. Total Estimated Cost of the Proposal

The following provides the breakdown of overhead costs and total estimated cost of the proposal. The total cost for implementation is estimated to be approximately $3,958,001. This total takes into account the cost for new employees to obtain their CRCM if they are not already certified.

IVdi. Breakdown of Total Estimated Cost

The following provides the breakdown of overhead costs and total estimated cost of the proposal. The total cost for implementation is estimated to be approximately $3,958,001. This total factors in the cost for new employees to obtain their CRCM if they are not already certified. That cost is included in the overall certification/ongoing training cost of $113,001.00. The ongoing total annual cost of $3,877,059.00, (excludes the cost of $80,942.00[12] to certify new employees). These totals are only an approximations to give an understanding of the relative cost of restructuring the department and they do not include other factors such as opportunities for cross training, automating processes and reporting, utilization of existing organization tools, etc., which can be considered to help reduce overall costs.

Overhead Item	Cost
Personnel	$2,490,000
Technology	$1,355,000
Certification/Ongoing Training	$113,001
Total Cost for Impementation	**$3,958,001**

Total Annual Cost	**$3,877,059**

[12] Refer to the table on page 49.

V. Non-Financial Impact

Va. Potential Hurdles

Implementing organizational change will take time and will likely be met with resistance especially with the current culture in the Bank. While compliance is not new to the organization, there are a few hurdles that should be considered. These may be summarized as resistance to change, inability to resource, and potential knowledge gaps.

Some of the current challenges include: FRBC and 1LOD working in siloes, instead of working collaboratively; compliance is seen as a deterrent to customer facing employees. Additionally, the 1LOD lacks QA/QC functions to ensure processes are adhering to lines of business policies and procedures. Furthermore, lines of business have a lack of documented guidelines and procedures. There are BURCs inserted for each line of business who are coordinators between lines of business and compliance. However, they do not function in a QA/QC function (which is regulatory requirement related to lines of business having a second review process) to self-identify compliance concerns. There is an overreliance for FRBC to conduct 1LOD QA/QC. However, compliance issues identified are negatively perceived as a bottleneck instead of improvement opportunities for the 1LOD. Introducing the concept of developing a risk control environment will likely be received with criticism and responded with compliance needing to do the work for 1LOD and develop risk controls for 1LOD. This type of resistance to change will diminish the ERM framework of 1LOD owning the risk and being proactive to identity and mitigate compliance risks.

An additional hurdle is the resourcing needed to support existing processes that are enhanced/expanded and the building of new processes. As a smaller institution who is focused on improving the efficiency ratio and minimizing expenses, this proposal may be seen as a challenge to deliver on improving the efficiency ratio. While there may be positive intentions, the additional reporting, required discussions, and on-going management and oversight may be perceived as either something most areas are currently doing; or the additions may be perceived as adding more to plates already full of expectations.

A third hurdle is the knowledge gap. While FRBC has recently hired a number of associates from mid to large size banks, the majority of the existing staff are homegrown compliance professionals who lack the industry knowledge. In addition, the bulk of 1LOD management consists of associates who spent the majority of their careers at Trustmark and lack the banking and compliance knowledge gained at larger institutions. The knowledge gap makes implementing the changes required for this proposal difficult to impose on an organization who is used to doing business a certain way.

Vb. Approach to Overcome Hurdles

In order to address the hurdles that were outlined this section will provide solutions to overcome roadblocks. An important element in overcoming the challenges is the delivery and approach in communication and creating a collaborative environment. This is central to aligning FRBC and 1LOD towards a common objective. Additionally, the ability of open dialogue can play a vital role on overcoming the challenges stated in the prior section and building a strong compliance baseline. Lastly, an understanding of the culture and customizing the approach can result in stakeholders being more open and receptive to change.

In response to the resistance of change from the 1LOD, communication from FRBC needs to clear and transparent. There needs to be a top-down approach where 1LOD executive and senior manager recognize the importance of compliance and the need for a more collaborative environment between FRBC and 1LOD. A working group consisting of key stakeholders from 1LOD and FRBC need to be created to identify areas that 1LOD and FRBC can improve and provide an environment where the two groups can work together. The resistance from 1LOD comes from the lines of business feeling that FRBC identifies compliance issues but does not provide support to assist in mitigating the risk. The working group will break down the current silos, provide 1LOD compliance support from FRBC, and keep 1LOD and FRBC engaged in the problem solving process. Additionally, the roadmap was constructed to introduce the change in a stepwise manner within a four year period and engage key stakeholders in the build. The engagement can result in stakeholders to have early buy in and provide ongoing adoption.

The obstacle of resourcing can be addressed through the working group being informed of the needs of the enhanced and newly created processes, and identifying other options that will not result in increasing expenses for the organization. This can include: cross-training employees, repositioning employees and increasing their level of responsibilities, or utilizing technology to automate manual processes. Since the roadmap will take approximately four years or longer (depending on constraints or externalities), there will be time for the organization to prepare for any additional expenses prior to the implementation of the restructuring. However, the working group is given the opportunity to demonstrate to the Board and executives that all options have been exhausted prior to requesting for additional resources.

The final obstacle of the knowledge gap can be addressed through training, sharing of knowledge, and participation in industry forums. As mentioned in the Strategy and Implementation section, FRBC is heavily invested in getting associates certificated in compliance and participate in ongoing training. Additionally, FRBC associates are attending conferences to network with peers in their industry. A similar thing is

occurring with 1LOD. The working group itself provides opportunities for participants to share their knowledge and expertise with each other. Also, there should be ongoing and more frequent interactions similar to this. For example: The line of business have their own committees and they allow compliance to have a seat on the table. FRBC has its monthly Compliance Committee, and they have the 1LOD BURCs participant and present. These types of interactions are key to sharing knowledge between 1LOD and FRBC, and by having associates who have worked in larger banks present and willing to share their industry knowledge is valuable in helping existing associates bridge their own knowledge gap.

Overall, in order to overcome these obstacles communication and collaboration are key. This will help 1LOD and FRBC understand the current environment, what is needed to improve and move forward, and keep key stakeholders engaged to support the delivery of this proposal.

Vc. Measuring Non-Financial Impacts

A bank that measures compliance effectively can prevent reputational damage, protect the bottom line, and potentially avoid costly fines and enforcement actions by establishing the right performance metrics. Compliance metrics can come from many potential sources such as culture surveys, risk assessments, disclosures, Compliance hotline, etc. It is important for FRBC is established compliance key performance indicators (KPIs) that measure employee engagement and awareness of the CMS program, how well the organization complies with rules and regulations, and ethical decision-making[13].

The following provides measures of success and effectiveness of the CMS program:

- Growth, understanding, and acceptance from the lines of business
- Lines of business effectiveness in managing controls relative to compliance
- Obtaining satisfactory ratings from Internal Audit and OCC exams.

The following provides example of how to measure the success and effectiveness of the CMS Program[14]:

- Number of times and how often policies and procedures are reviewed and/or updated
- Number and nature of policies violations
- Culture surveys and knowledge assessment results
- Evaluate compliance completion rates for training, reviews, testing, and addressing regulatory issues

[13] Onetrust.Maxwell, Kelly.*"Compliance program performance metrics: How to measure compliance. https://www.onetrust.com/blog/compliance-program-performance-metrics/.September 7, 2022*

[14] Onetrust.Maxwell, Kelly.*"Compliance program performance metrics: How to measure compliance. https://www.onetrust.com/blog/compliance-program-performance-metrics/.September 7, 2022*

- Evaluate the reach, medium, frequency, and engagement rate of compliance communications
- Frequency of compliance training program updates
- Post compliance training results
- Number and nature of incidents by employees who have completed training
- Reporting rates for ethics complaints (anonymous and non-anonymous)
- Retaliation report trends, include the number of reports of retaliation
- Evaluate internal audit and regulatory reports that were given unsatisfactory ratings and evaluate issues on the report (number and nature)

In order to understand which compliance KPIs need to be priorities, there needs to be an understanding of the data that is available. There are sources of untapped data in HR, from the sales team, etc. that the compliance program can use to gain a deeper understanding into issues such as brand reputation, silent retaliation, compliance deficiencies, etc. Then, it is a matter of taking each data point in context to understand how to interpret it and to evaluate how it is relevant to the compliance program goals and regulatory requirements[15].

To measure the awareness of compliance expectations, the Bank can consider implementing an employee questionnaire to the lines of business. The first response set can form the baseline to assist in prioritizing areas that compliance can improve upon. From a customer perspective, the Bank can utilize its customer complaints information and social media commentary to assess particular topics of experiences that rise to the level of compliance attention, particularly topics that may be associated with high compliance risk (i.e., discrimination, unfair treatment, unethical behavior, etc.). Finally, the Bank can consider implementing customer surveys that are similar to the employee questionnaire; example question around customer experience and satisfaction. These insights allow for more effective allocation of resources, tell a more compelling compliance story to executives and the Board, and results in a better compliance culture.

[15] Onetrust.Maxwell, Kelly.*"Compliance program performance metrics: How to measure compliance. https://www.onetrust.com/blog/compliance-program-performance-metrics/.September 7, 2022*

VI. Conclusion

In summary, the proposal to restructure the Bank's CMS program, enabled through the implementation of the phased approach is beneficial to the Bank in both the near and long term. The current work taking place to fix existing processes and the proposal to create new processes puts the Bank in a position to further understand its key compliance risks and leverages best practices to address them in a holistic manner. It creates a baseline on which the Bank can continue to expand its Company footprint and adapt to the changing regulatory environment, where regulatory scrutiny continues to increase. This will allow the Bank to better manage compliance risk across the organization. Lastly, it will lead to a better compliance culture across the organization and a better equipped the organization to address risk. This will also align the Bank's CMS program to industry standards and best practices.

The build will take time and resources from the Bank, but there is a compliance foundation to continue building upon. Leveraging communication and collaboration between the lines of business and compliance through a working group will provide engagement from all key stakeholders and effective challenge across the organization that will help in the initial stand-up; as well as ongoing sustainability and expansion of the program. The establishment of KRIs and ongoing communication will help frame future priorities and program evolution to support the Bank's strategic initiatives and agenda. Lastly, the proposal is intended to elevate the existing CMS program and make it suitable for a mid-size level bank which in turn will also provide for a more effective ERM framework.

VII. Bibliography

1) American Banker Association, *Certified Regulatory Compliance Manager Online Prep Course: FIRREA Civil Money Penalities,* 2023

2) Ballard Spahr. Culhane, John L., Larson, Kristne E.,*"CFPB and OCC announce consent orders with Bank of America involving deposit account representment fees and credit cards."*, 2023

3) CFPB, "*CFPB Takes Action Against Bank of America for Illegally Charging Junk Fees, Without Credit Card Rewards, and Opening Fake Accounts."*, 2023

4) Consumer Compliance Outlook 2019, *Promoting Effective Change Management*. Viewed 10 October 2023, <https://www.consumercomplianceoutlook.org/2019/second-issue/promoting-effective-change-management/>

5) Engineess 2021. *How to Conduct a Technology Assessment: A Four-Step Guide*. Viewed 25 October 2023, <https://www.enginess.io/insights/how-to-conduct-technology-assessment?l=en-us>

6) Onetrust, Maxwell, Kelly 2022, *"Compliance program performance metrics: How to measure compliance".* Viewed 25 October 2023, <*https://www.onetrust.com/blog/compliance-program-performance-metrics/*>

7) Whistleblower Security 2023, 6 Tips for Developing a Culture of Compliance. Viewed 25 October 2023, <https://blog.whistleblowersecurity.com/blog/6-tips-for-developing-a-culture-of-compliance>