# *Stonier Capstone Project*

## *Creating an Integrated Enterprise Risk Management Framework*

Due: Tuesday, March 1, 2022

Submitted by:

Jennifer P Schmidt

Burke & Herbert Bank

Submission Date:  February 3, 2022

# Table of Contents

## Executive Summary

Safe and sound bank operation.  Customers expect it.  Regulators demand it.  Leaders own it.  Headlines highlight the importance of strong risk management practices, or lack thereof, at financial institutions.  News stories and regulator press releases note language such as unsafe and unsound banking practices; deficiencies in enterprise-wide risk management; failure to maintain adequate internal controls; failure to establish effective risk assessment processes; and failure to correct the deficiencies in a timely manner.  These headlines bring with them a cost, often in the form of penalties and typically complemented by the cost of building or enhancing a financial institution's risk management program.

The pace of change in risk management is increasing. Risk events such as cyber and ransomware continue.  Risk types are also evolving, as seen by recent focus on climate, environmental, social and governance risks.  These emerging risk areas couple with more traditional focus areas (*e.g.*, credit, financial, and reputation risk) to highlight the evolving scope of risk management practices.

The intent of this capstone project is to build the case to start the Enterprise Risk Management ("ERM") journey at Burke & Herbert Bank ("Bank"), specifically implementing a risk management baselining effort.  Creation of an integrated ERM program, enabled through the baselining project is beneficial to the Bank in both the near- and long-term.  Research within this paper supports this journey; this summary shares several supporting observations.

Regulatory scrutiny is on the rise.  This interest is not only evidenced through the headlines noted above, but also through the Bank's own experience with annual safety and soundness exam processes.  Examiners are requesting ERM policies and procedures, risk appetite statements and assessments and Board-level risk management minutes.  By starting the

baselining effort now, building and expanding upon existing practices, the Bank has the opportunity to create its narrative for a holistic risk management approach. Evolution and enhancement will follow, but the baseline enables the Bank to start its journey.

Evolving expectations are not new to the Bank, which at $3.55B as of June 30, 2021 and 169 years of continuous operation has experienced change throughout its decades of service. As the Bank looks to its future, it plans for growth by extension of its market area beyond the northern VA footprint, with development of new products and services and through potential organization expansion. Strong risk management practices support these growth objectives as the Bank will have an understanding of its strengths and opportunities, creating clarity into areas where focus may be needed or be of benefit. Further, they will allow the Bank to be nimble as growth opportunities emerge. The Bank is not starting from scratch, but rather has the ability to build upon its currently distributed risk management practices to create an integrated approach.

The baselining project can be described as a cycle of four key steps, woven together through two key supporting processes. The project leader will guide the effort, which will begin by creating a risk inventory, working with business leaders across the organization. Next, synthesis and prioritization will yield the key risks toward which the Bank should focus its attention. That attention can be directed through the next step in the cycle, the development, reporting and discussion of results as evidenced through risk metrics. Through dialogue and understanding key risk performance, leadership can make remediation or acceptance decisions. This cycle is not once and done, but rather continues as an on-going process as the business environment, both internal and external evolves. In addition, this cycle must be supported through open and on-going communications, through defined forums and routine business operations. This dialogue, including effective challenge ensures conversations occur at appropriate levels, with risks clearly understood – both in how they impact a particular area and how they may connect with other areas – and decisions are informed based on collective insight.

The project will require organization engagement with Bank leadership setting the tone of its importance. Bank management efforts will include both current and potentially expanded expectations in risk identification and management as well as mitigation and acceptance decisions. Team members will also engage as they manage risks through their daily activities.

This project is important to the Bank, from a value preservation standpoint as well as organization and customer perspectives. Based on the headlines above and as discussed in this paper, project execution could preserve between $262k and $1.5M, if regulatory penalty ratios (*i.e.*, penalty to asset size) are unchanged. As time progresses, it would not be unlikely for the amounts to increase. There is cost associated with implementing the project, both opportunity (*i.e.*, team members focused on this project are not focused on other priorities) and incremental (*i.e.*, training, new team member); however, the value preserved likely outweighs this spend.

This project may be met with some resistance, but with focus these hurdles can be managed. The organization, which currently manages risks in a distributed manner, may be resistant to centralized oversight; an ERM approach may be seen as ceding responsibility. In addition, there may be an inability to resource the effort, given other competing efforts. Further, while willingness and commitment may exist, there may be skill or knowledge gaps to manage.

Similar to an enabler of on-going risk management practices, communication is critical to overcoming these organization challenges. Engaging team members in building the solution, leveraging their experience to integrate elements from current distributed processes into the overall outcome and offering training where it may be of benefit can all contribute to enhancing both a culture of risk management and an engagement in on-going delivery of ERM needs.

The risk management culture enabled through the baselining project will likely include an awareness of the importance of risk management to the organization, utilization of a common vernacular and management and application of metrics to guide decision making.

Awareness creates clarity of expectations, both for individuals and for interactions across the organization. Similarly, common vernacular enables understanding, limiting potential misinterpretation. Metrics allow grounded, data driven decisions to guide risk acceptance and remediation priorities. Together, these culture elements support enhanced job satisfaction (*e.g.*, through role clarity), more predictable process outcomes and process delivery and less confusion for the organization and customers alike. A key beneficiary of these risk management efforts is the customer, as positive experiences likely lead to on-going and potentially deeper relationships over time. This benefit accrues to the Bank over time as well, as customers are a key element to the organization's growth engine.

In summary, implementation of a risk management baselining project to begin the ERM journey is valuable to the Bank in both the near- and long-term. Starting the process now allows the Bank to build now and evolve over time. Through an understanding of strengths and opportunities, the Bank can prioritize efforts to support continued operation and future growth goals (*e.g.*, it may be more nimble as acquisition / expansion opportunities come to be). Efforts now also allow the Bank to own its narrative and journey, investing at a pace and time of its choosing. These efforts drive value for the organization and its customers, through consistency in process, rigor in decision making and ultimately a stronger resulting customer experience. They mitigate, although do not fully eliminate risks related to the environment in which the Bank operates. While there is cost associated with the effort, the benefits likely outweigh the investment.

## Introduction and Background

### *A Brief History*

Burke & Herbert Bank ("Bank") is rich in history, as the oldest community Bank in northern Virginia.[1] The 169 years of continuous operation are core to the Bank's history and its future, a future that is focused on long-term stability. Its success lies in its customer service and conservative approach to banking, which together serve the local community while managing risk to enable a platform for on-going operations.

The $3.55B Bank operates 24 branches, with 23 in northern VA and as of August 2021, one in its expanded footprint of Fredericksburg, VA. This expansion also included opening a Loan Production Office. The expansion marks the Bank's first physical presence outside of northern Virginia.[2] See Appendix A for a map of the Bank's branches and target market.

The Bank offers an array of banking products and services aimed at meeting personal and business customers' deposits, lending and investment needs. Products include checking, savings, money market and certificate of deposit accounts; mortgage and consumer loans and lines of credit; business loans and lines of credit; wealth management, trust services and private banking. In addition, debit and credit cards are available to both personal and business customers. Further, the Bank offers a range of services to business customers, from wires and ACH to remote deposit capture. Customers can access the Bank's offerings through traditional branch and in-person interactions, by customer contact center and phone inquiries and, as has been and is expected to continue to be the case across the industry, through increased use of digital channels, including mobile and online banking.[3]

---

[1] https://www.burkeandherbertbank.com/about/
[2] Ibid
[3] https://www.insiderintelligence.com/insights/digital-banking-trends/

### ***Location, Business Model and Strategy***

The Bank delivers its "exceedingly conservative business strategy"[4] across its footprint. Its strategy is one of independence enabled by growth, operational efficiency and people development. Its 2020-2022 priorities align with the strategy, with goals to enhance efficiency in revenue generation; enhance/maintain customer experience; efficiently manage risk to acceptable levels; improve organizational efficiency; and enhance/maintain employee experience.[5]

This overarching strategy continues to propel the Bank. Planning efforts for 2022-2024 are in process and expected to continue to consider people, process and technology in support of business growth. While not finalized, strategic priorities may also evolve. For example, the Bank may target additional geographic expansion for growth rather than only deeper penetration within existing markets. Also, in addition to targeted product growth, fee-based income may become an area of focus for revenue growth. Finally, the Bank may aim to transform its digital capabilities given expected continued customer demand for the offerings.

### ***Financial Position***

As of June 30, 2021, the Bank's assets total $3.55B, up from $3.33B as of June, 30, 2020.[6] During the same period, the loan portfolio decreased from $1.97B to $1.78B, noting the challenging lending environment given competition and COVID-19. Deposits increased from $2.71B to $2.91B, demonstrating strength; however, given the current low rate environment and the weak loan demand, the utility of deposits to earnings is historically weak. Excess liquidity has been used to grow the securities portfolio, which increased from $890M to $1.38B.[7]

---

[4] Williams, Julia, *Burke & Herbert Celebrates 150 Years A living legacy of Commitment and Service.* (Richmond: The Dietz Press, Inc., 2002), 4.
[5] Burke & Herbert Bank. (2020) Town Hall 1_21_2020 Final. Unpublished internal company document, 15.
[6] https://www.burkeandherbertbank.com/wp-content/uploads/2021/07/Q2_2021_Financials.pdf, Page 2
[7] Ibid

Review of quarterly financial performance for periods ending June 2020 and June 2021 shows interest income remained relatively flat at $25M, with the decrease in interest from the loan portfolio offset by an increase in interest from securities. Interest expense decreased, primarily driven by reductions in deposit product rate offerings; however, with the current rate environment, further reductions are not anticipated. Non-interest income increased nominally, while non-interest expense increased based on increasing personnel costs to fuel product and service growth and geographic expansion. The primary driver of income growth was improved provision for loan losses. In June 2020, the economy faced uncertainty with COVID-19; as such, the Bank applied its conservative credit risk management approach to its provisioning levels. As the pandemic continued to play out, these provisions decreased. Noting the rate environment, non-interest income and expense management are expected to be key to future earnings growth. [8]

***Competition***

Burke & Herbert Bank competes in the densely populated northern Virginia market. Competitors can be evaluated from several dimensions, including deposit share, commercial and mortgage lending. As of June 30, 2020, Burke & Herbert Bank was ranked 16th with a 0.86% deposit market share in the Washington-Arlington-Alexandria, DC-VA-MD-WV metropolitan statistical area. Banks with greater market share tend to be national-presence institutions (*e.g.,* Capital One, Bank of America) and some community banks (*e.g.,* Eaglebank, Sandy Spring). Deposits are concentrated in the region, with the top 9 banks comprising 81.5% market share.[9]

An August 2021 survey of Bank leadership noted commercial lending competitors range from community banks to larger institutions. For Commercial Real Estate ("CRE") loans, the

---

[8] https://www.burkeandherbertbank.com/wp-content/uploads/2021/07/Q2_2021_Financials.pdf, Page 3

[9] https://www7.fdic.gov/sod/sodMarketBank.asp?barItem=2

Bank primarily competes with community banks; with Construction & Industrial ("C&I") and Small Business lending, the Bank competes with the gamut of financial providers.

In Mortgage Lending, the Bank's competitors extend beyond its geographic footprint. Based on 2020 data, the top five mortgage lenders in the United States are Rocket Mortgage, United Wholesale Mortgage (located in Pontiac, MI), Freedom Mortgage, Wells Fargo and loanDepot.[10] In the local Washington DC metro region on a 2020 loan volume basis, the top five mortgage lenders include Wells Fargo, Intercoastal Mortgage LLC, First Savings Mortgage Corporation, McLean Mortgage Corp. and Atlantic Cost Mortgage LLC.[11] These lists indicate that online capabilities exist in mortgage lending, as do offerings through large and small traditional banks and focused mortgage lenders.

***Current and Evolving Risk Management Environment***

The Bank currently manages risk in a distributed model, with responsibilities delivered by business units, largely along functional lines. The Bank relies on various policies and committees to manage different types of risk (*e.g.*, financial, strategic, reputation, compliance, and operations risk). For example, the Chief Credit Officer is responsible for credit risk and related Loan Committees; the Chief Financial Officer has Asset-Liability Management ("ALM"), Investments, and Interest Rate Risk Hedging and chairs the ALM Committee.

While several leaders have a role in risk management practices, there is opportunity to clarify who is responsible for and allowed to decision risk acceptance, to what level and at what time. Notably, the Bank's likely priorities to grow its footprint and digital offerings may lead to it becoming a more complex institution. In addition, exams and regulator inquiries are evolving,

[10] https://www.housingwire.com/articles/here-are-the-top-15-mortgage-lenders-of-2020/
[11] https://www.bizjournals.com/washington/subscriber-only/2021/04/09/largest-home-mortgage-lenders-in.html

with specific requests for Enterprise Risk Management ("ERM") policies, risk appetite statements, risk assessments and board-level risk management minutes. Their questions demonstrate the importance being placed on effective risk management practices.

Taken together, the Bank's goals and the regulatory environment suggest an integrated approach to risk management may be both important and beneficial to the organization. An ERM framework has the potential to establish norms to manage risk holistically, enabling efficiencies and driving collaboration. It may guide the design of supporting tools, including articulation of roles and responsibilities, expectations of documentation such as process flow and risk appetite, and on-going evaluation of risk, including assessments, measurement and potential acceptance and/or corrective actions. Finally, it should create clarity of risk governance and how enterprise level decisions may utilize the information, for both corrective action and advantage.

## Strategy and Implementation

### *Change for Consideration – Building a Baseline ERM Framework*

The goal of this process change is to establish the baseline from which an integrated ERM approach can begin and evolve at the Bank. Building an ERM framework requires an understanding of where the Bank wants to go and recognition that the effort will be a journey. The Bank can consider using the OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches[12] to guide its efforts. However, efforts need to recognize the applicability of these guidelines (*i.e.*, banks at greater than $50B in assets), Burke & Herbert Bank's current size and complexity and its future goals. Essentially, the Bank can start "small" and build, as appropriate.

[12] https://www.occ.gov/news-issuances/federal-register/2014/79fr54518.pdf. Pages 29 – 33.

A targeted risk management baselining project will guide the development of this process change. At the core, there are four key delivery elements, complemented by two supporting processes. The four elements include the following: 1) Understand the Bank's risks by establishing a risk inventory; 2) Prioritize risks to identify the key risks to achieving both the Bank's strategic plan and on-going safe and sound operation; 3) Measure results based on defined performance metrics for each key risk, leveraging and building upon current reporting; and 4) Remediate or accept, as deemed appropriate. These four steps are not the end. The process needs to continue as a cycle, where risks are reviewed and updated based on the evolving internal and external business environment. Perhaps most importantly, communication and governance norms are essential to building, measuring and maintaining on-going understanding of the risk environment. A September 2021 Executive survey noted use of strong communication and simple technology (*e.g.*, Excel) rather than a large scale governance, risk and control solution would support the Bank in effectively beginning its ERM journey.

***Rationale and Project Implementation Leadership***

As discussed in the Introduction, the Bank currently manages risk in a distributed model. While processes exist and risks are generally understood within each business vertical, there is an opportunity for communication and cross-pollination to inform decision making. A recent product launch demonstrates the need for this integration of risk discussions – Mortgage Lending developed and rolled out a product without final Compliance approval. While Compliance had been engaged in early discussions, the Lending Team did not share the final program document until after launch, and only after Compliance learned of the launch due to a Marketing Team request for a review of product advertising materials. While the product design met most of the regulatory needs, there were opportunities to enhance the Bank's documentation.

The teams worked together to remedy the needs on the back-end; however, the effort required rework from Lending and Marketing that could have been avoided with earlier and on-going communication. This example also highlights that decisions made by one team can create risk in other teams, perhaps unknowingly. Open communication, including rigorous review of product impacts can help get ahead of this challenge. Finally, this example notes that risks are not individual, but they are potentially multiplicative and often positively correlated. In this case, the Lending team aimed to minimize strategic risk, by launching a product as outlined within the strategic plan; however, the decision created potential compliance and reputation risk. The teams were able to mitigate the risks, once known; however, the example highlights that as a Bank, management may not have a complete handle on the collective risks it is managing.

This situation is not one on which to dwell, but it leads to a very particular question – does the Bank understand its key risks, the ones that without mitigation could negatively impact the safe and sound operation of the organization? Further, without conversation, does the Bank know if it is taking on more, or less, risk than it actually desires?

The Bank is not starting from scratch to address these questions, but rather has an opportunity to build on efforts from several areas that may be further along the maturity curve. For example, the Compliance Management System at the Bank is generally strong. The team conducts an annual risk assessment, with engagement from business lines; results inform work priorities from policy and procedure updates to training curriculum to Level 2 (*i.e.*, second line of defense[13]) scope and frequency objectives. The team communicates results and partners with business lines to mitigate risk opportunities. The team also engages in project support, offering subject matter knowledge and delivers ad hoc training, should areas of concern in performance

[13] https://www.occ.gov/news-issuances/federal-register/2014/79fr54518.pdf. Pages 29 – 33.

arise. Finally, the team maintains a strong pulse on the regulatory environment, evaluating potential impacts of changes and working with business lines to support compliance by the effective date. This programmatic approach leads to focused conversations across the Bank to support mitigation of compliance and reputation risk. This assessment, communication and partnership model is one that can apply more broadly in the Bank's risk management efforts.

Financial risk management and credit risk management practices also provide a lens into the potential framework. Interest rate, liquidity and market risk processes are in place, with metrics guiding discussions and decision-making. The use of metrics to inform discussion and decisions is another element that may apply more broadly in risk management efforts. In addition, recently established review and attestation processes associated with Internal Controls over Financial Reporting utilize clear accountabilities, expected control performance through documented process flows and regular communication through Committee discussion.

Bank Secrecy Act ("BSA") processes leverage technology to support efficient and effective delivery of regulatory requirements, making processes more efficient and creating greater assurance of compliance. Periodic metrics and management reporting ensure awareness of issues to drive focused remediation (*e.g.*, Customer Information Program exception reporting).

These examples collectively point to elements of a strong risk management program – defined processes, including roles and responsibilities and use of technology where meaningful; assessment of risk in those processes and use metrics and management reporting to evaluate performance; and communication and partnership in decision making and remediation activities.

Achievements expected from a structured, integrated risk management approach include an understanding of key risks, their overlap across various business lines and the potential impact of the risks. Individual business lines will still own and manage their risks, particularly the technical depth and detail. However, creating visibility across the risks through reporting and discussion among leaders will support a clearer understanding of connectivity of risks and an overall ranking of the Bank's key risks. With this information, the Bank can prioritize its management, acceptance and mitigation efforts. For example, implementation of a technology solution may mitigate both a compliance and reputation risk currently handled through manual processes; understanding customer impact and financial impact can further guide these remediation and/or acceptance decisions, particularly relative to overall Bank priorities.

Communication of issues and opportunities leads to efficient resource allocation, likely reducing rework as on-going dialogue mitigates an issue from occurring. Overall, the Bank can anticipate greater cultural awareness of the importance of effective risk management.

Implementation of the framework to understand, prioritize, measure, remediate and communicate risks will require the project leader to meet with senior risk owners on a regular basis. Initial discussions will focus on baseline goals and potential training needs, and will then move to facilitation of the risk identification process, including defining the risk categories the Bank will use to manage risk (*e.g.*, credit, operational and emerging risk areas such as environmental, social and governance ("ESG")). From there, efforts will focus on aligning risks to those categories and understanding current management practices. The project leader will be responsible for initial data gathering and synthesis, essentially creating the risk inventory, followed by review and prioritization discussions with the same group and Bank senior leadership to define key risks. While metrics will be defined and managed by risk owners, the project leader will establish communication mechanisms to enable discussion of performance. The individual business line risk metrics and reporting will be a key input to dialogue, enabling clarity of risk performance at both individual and aggregate levels. Discussions will likely occur through a new committee structure, chaired by the project leader as part of a new set of on-going responsibilities. The project leader will work with senior leaders to assess initial rollout and early progress to adjust and align enhancements to the Bank's needs. The overarching outcome is integration of this committee into the Bank's overall governance norms, with a regular meeting cadence and reporting standards, enabled by a culture of risk management.

***Alignment with Business Strategy***

A September 2021 Bank leadership survey noted an expectation for Bank growth in the coming 2-3 years, with the resulting organization anticipated to look quite different from today. Specific growth engines noted include geographic expansion, new product and service offerings (*e.g.,* medical/dental commercial lending product and increased digital capabilities) and potential acquisition, in alignment with existing products and services as well as extensions of those offerings. While growth creates advantages, it also needs to be carefully managed to ensure continued safe and sound banking practices.

Strong risk management practices support each of the Bank's growth objectives. For example, geographic expansion may bring additional financial risk as well as compliance risk (*e.g.,* new states may have different rules and regulations) and reputation risk. New products and services may create operational, compliance and reputation risk depending on how and to whom the offerings are delivered. Acquisition objectives may create risk across each of the key areas – strategic, financial, compliance, operational and reputation risk; they may also require the Bank to move quickly. A baseline understanding of key risks and performance allows the Bank to be nimble as growth opportunities present themselves. An understanding of internal strengths and opportunities can also help guide due diligence evaluations (*e.g.*, synergy in control processes; areas that may require bolstering). Further, this awareness can provide clarity into the Bank's current skill sets and the areas it may need support from outside consultants to manage delivery. In each of these cases, identification, measurement and communication will help leaders assess potential overlap of risks and enable appropriate dialogue to address or accept the results.

The Bank's collective growth objectives may require a pace of change that relies on an already-understood risk posture with well-defined review processes.  Baseline efforts will support this goal, with delivery of an established risk inventory and defined processes to support review of on-going changes to the risk environment.  As growth catalysts occur, the risk assessments can evaluate those events in concert with the overall system.

Critical to the successful implementation of the baselining effort and to building an overall risk management approach is Bank culture.  The September 2021 Executive survey noted that team members care about the Bank, its customers and each other.  The survey indicated the Bank's opportunity to harness its existing culture to advance the risk management environment. It highlighted the recent successful launch of the review and attestation processes associated with Internal Controls over Financial Reporting, noting two key success drivers of the success: leadership set the tone that it is both acceptable and expected to call out risks and address issues; and team members participated actively and openly in regular Committee discussion.  It noted additional examples of the Bank culture, including business line escalation of self-identified issues (*e.g.*, to Compliance, Operations and Finance) and requests for remediation support from partners.  These interactions have in many cases helped the Bank address root cause issues before they became pervasive.  In the baselining risk efforts, these issues would be included in reporting and committee discussion, based on materiality (*e.g.*, dollar) or potential pattern of practice (*e.g.*, isolated versus often occurrence) thresholds.  Thresholds will allow management to consider the substantial or systemic impacts of risk issues rather than each isolated instance.

The Bank's growth objectives may also create new or increasing regulatory compliance requirements. For example, focus on digital delivery elevates expectations from the perspective of The Electronic Signatures in Global and National Commerce ("E-Sign") Act and other regulations which cite electronic delivery compliance with E-Sign (*e.g.,* Regulation DD – Truth in Savings; Regulation Z – Truth in Lending). Creating a forum for communication of strategic objectives and discussion of risk associated with implementation will help in both identifying and addressing these requirements prior to launch, minimizing rework after launch. A 2021 article on the importance of compliance, risk and business lines working together noted, "Risk doesn't respect borders. Consider compliance risk…violations can have reputational, financial and regulatory consequences that impact much more than the compliance department."[14]

Beyond individual regulation expectations, the Bank's strategy may also lead to broader regulatory risk management expectations. As the Bank grows and diversifies its products, services and locations, regulators will expect it to clearly understand risks to delivery. The Bank is in a position to define and implement its framework as it grows; creating the key risk baseline and management norms now will support this evolution.

The September 2021 Executive Survey also noted that understanding risks and mitigation needs would also serve the Bank's customer service approach to banking. With a business objective of differentiated customer service, the Bank needs to understand where it may be potentially creating reputation risk. Understanding these risks and drivers and managing potential acceptance and mitigation will be important to the Bank's strategy as customers will contribute to continued business success; without it, the Bank may impede its growth objectives.

[14] https://www.ncontracts.com/risk-and-compliance-together, Page 3.

Overall, each of the Bank's growth objectives, as well as delivery of current operations can benefit from on-going, repeatable processes which include open communication to support decision making.  Per the September 2021 Executive Survey, this open communication establishes clear team member roles and responsibilities, aligns activity and creates efficiency in delivery as people are moving in a similar direction.  Further, it helps to focus the energy and efforts of team members on the risks that matter; that is, the risks that may impede delivery of the strategic plan as well as safe and sound operation.  It helps in management of potential blind spots in any one area of the Bank.  The on-going dialogue not only builds point-in-time knowledge, but also builds skills to assess and understand impacts of future contemplated changes.  Finally, it can guide inquiry of various risks and situations, essentially building the competency of effective challenge across the organization.

It is important to note that risk management processes will not prevent all potential issues from happening.  However, establishing processes that enable identification, measurement and communication of risk and building a culture that embraces risk management will ensure that when an issue is identified, it can be appropriately addressed. In addition, this foundation should also help the Bank to become more efficient in its risk practices, enabling it to react more quickly as the speed at which risk happens today continues to increase (*e.g.*, cyber-attacks) and the type of risks banks are managing continues to expand (*e.g.*, climate change).

### ***Future Opportunities***

Building risk management into the governance and infrastructure of the Bank begins with this baselining effort.  The project sets the stage to support successful current operations as well as future organization growth.  Baselining risks enables the Bank to understand its strengths and opportunities across processes, technologies and skill sets. It also enables the Bank to be nimble if and/or when opportunities emerge (*e.g.*, potential acquisition targets, expansion locations). Further, baselining efforts allow the Bank to own its story from a regulatory risk management standpoint, creating the ability to offer context to its risk framework, management routines and action planning processes. The project also allows the Bank to learn through implementation, build on practices and enhance its capabilities. As the Bank continues to grow, and as structure or governance models change, its ERM process and capabilities can continue to grow and mature based on the experience with the initial build and an understanding of on-going needs.

Implementation of the baselining project will include design of risk management governance models. These models will likely include a Senior Risk Management Committee, during which key risks, metrics and decisions will be discussed. In addition, committee sub-groups may be established or enhanced to support on-going decisions. Finally, a Board-level committee will likely be formed to create oversight and enable understanding of how the Bank is managing its risks holistically. Each of these committee structures is likely to evolve over time.

Rollout of the implementation framework and supporting governance models creates an on-going cost commitment. As this integrated approach is new to the Bank, financial investment will be needed to build the team to deliver the baselining efforts and on-going risk management routines, including facilitation of risk identification and periodic review processes. This budget is not a once-and-done line item, but will continue to be a cost to the Bank over time.

As the Bank grows and potentially becomes more complex, additional costs may also emerge. Processes will need to evolve and advance; technology may become a more central element of the risk management approach; and additional personnel costs may become a priority to support on-going maturity.

Finally, the Bank will need to consider personnel and staffing to support the on-going delivery of risk management processes. These considerations include overall organization structure and reporting lines, resourcing needs with the risk management team and within business lines and talent management and succession to planning enable on-going delivery of the processes established as part of the baselining project.

***Process Improvement Elements***

The key process improvement expected from the baselining project is enhancement of the Bank's overall approach to risk management. The new integrated approach will leverage current practices from several areas of the organization. However, the process, which will include interaction models and norms is expected to foster enhanced communication and cooperation, reduce redundancy and create efficiencies in delivery.

Bank leadership and risk owners will discuss key risks and performance through a newly established risk forum. Insights may lead to defined priorities, which may include new approaches to mitigate or navigate risk. Additional forums may be created or existing ones enhanced to support on-going communication and decision making (*e.g.*, new products and services discussions). A further outcome may include risk acceptance; however, these decisions will be broadly informed, an enhancement from current decision-making practices that may occur in business siloes. Essentially, a key benefit from this project will be the ability to inventory and aggregate risks holistically (*i.e.*, across the Bank) and rank them to influence decision making. The enhanced process and open communication will support team member alignment to common goals. It will also create the ability to leverage and build-upon existing thinking, enabling on-going learning throughout the team.

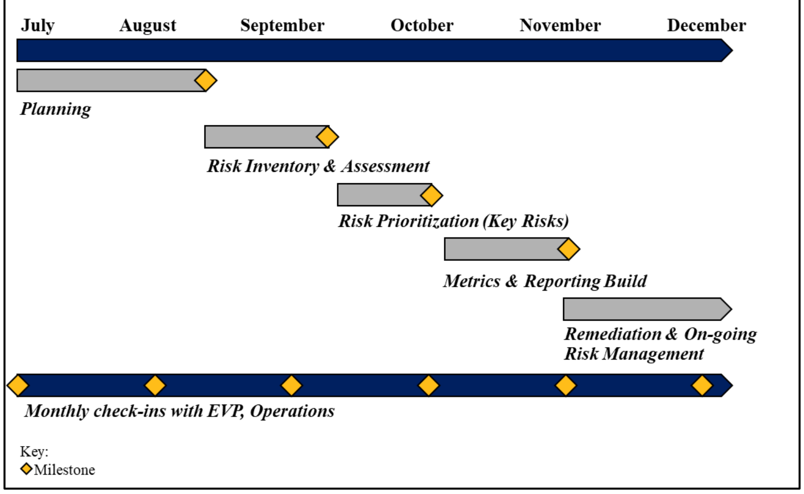
In addition to the risk management process, action plans may be put in place, many of which will align to business process change and/or improvement efforts.  For example, current manual processes may be targets for process improvement by understanding and remapping steps and roles.  Some manual processes may be enhanced more dramatically through technology. These outcomes would be informed through the risk committee process, enabling clear decision-making and resource allocation.  Business leaders would also share results of improvement efforts at the risk committee; this information sharing would likely lead to additional learning and further application of business process improvement approaches.

### ***Implementation Planning***

A structured approach to implementing the risk management baseline project will help guide progress. Figure 1 provides a summary view of the schedule.  While the roadmap begins in July, the dates are illustrative of the estimated duration of each stage, regardless of start point.

**Figure 1.  Implementation Roadmap**

*(Dates not final but illustrative to demonstrate likely duration of key roadmap elements)*




Detailed elements of each of the project implementation steps, including general timeframes and responsibilities are noted below:

***Planning (Project Leader, "PL") – 4-6 weeks***

- Kickoff with CEO and EVP, Operations ("EVP, Ops")
- Define key terms (*e.g.*, ERM, key risk, risk acceptance)
- Establish starting point risk categories
- Develop facilitation tools (*e.g.*, interview guides, assessment framework/grid for inherent risk, mitigation ratings and residual risk)
- Identify participants, including senior leadership team ("SLT"), risk owners ("RO")
- Gain agreement from CEO and EVP, Operations
- Communicate plan and goals to participants

***Risk Inventory & Assessment – 4-6 weeks***

- Facilitate individual discussions with risk owners *(PL, RO)*
- Integrate for cross-organization discussion *(PL)*
- Facilitate integrated session to identify potential overlaps, likelihood and impact of risk event, in both normal operations and stress scenarios *(PL, RO)*

***Risk Prioritization (Key Risks) (PL) – 3 weeks***

- Analyze to establish key risks; conduct follow-up as needed
- Conduct alignment meeting with CEO, EVP, Ops, SLT and RO ("participants")
- Finalize key risks and next steps

***Metrics & Reporting Build – 4 weeks***

- Establish / leverage current metrics to communicate performance *(RO)*
- Define and communicate Risk Committee approach, including agenda, roles and meeting expectations; establish integrated dashboard to assess performance *(PL)*
- Execute initial meeting and note enhancement opportunities *(PL, participants)*

***Remediation & On-going Risk Management (PL, participants) – On-going***

- Execute on-going discussions
- Track agreed-to remediation
- Assess impacts of accepted risks
- Gauge progress for further program element rollout (*e.g.*, risk appetite, risk limits)
- Prioritize on-going enhancements for delivery

**Financial Impact**

***Investment Size and Type***

The project investment required focuses on personnel costs driven by Bank team, Bank management and Board member time as well as a new team member to facilitate build and on-going risk management needs.  Specific cost drivers include incremental time for discussions with the project leader to identify, document and review prioritized key risks.  On-going costs may tie to participating in a new Management-level risk management forum, other potential forums and preparation of metrics and reporting.  Bank management cost drivers relate to review of key risks and reporting as well as participation in the risk management forum.  However, these incremental costs will likely be minimal as leadership currently reviews metrics and reporting to evaluate performance and opportunities.  Board of Directors costs align with the creation of a new Board-level ERM Committee, although these costs may be neutral if the Committee supplants an existing forum.  Finally, a new team member may support the build and on-going delivery; the presented estimate will include the full cost for a conservative view.

Notably absent from the financial cost estimate is a technology investment.  This blank line item is intentional.  As noted in the Strategy and Implementation section, given the Bank's size and overall goal of getting started, the risk management process will begin by using strong communication practices and simple technology (*e.g.*, Excel) rather than a large scale governance, risk and control solution. As the Bank builds its risk management capabilities, it may elect to evaluate technology solutions. These solutions would likely support further organization growth, expanded governance structures and heightened risk management processes. For now, people costs will be the driver of the required starting point investment.

***Financial Estimates***

Financials can be evaluated from an external environment review, informing value preservation estimates as well as through internal review of resource spend. The regulatory environment continues to increase expectations of effective risk management. Recent examples of fines paint a picture that investments, now or later are expected; if later, costs may include both the internal build as well as regulatory fines. Several 2020 and 2021 headlines highlight the seriousness with which regulators are approaching ineffective risk management practices.

In October of 2020, the Office of the Comptroller of the Currency ("OCC") assessed a $400M civil money penalty against Citibank, N.A. related to deficiencies in enterprise-wide risk management, compliance risk management, data governance, and internal controls.[15] In November of 2020, the OCC assessed a $250 million civil money penalty against JPMorgan Chase Bank, N.A. based on the bank's failure to maintain adequate internal controls and internal audit over its fiduciary business.[16] In August of 2020, the OCC assessed an $80 million civil money penalty against Capital One, N.A., and Capital One Bank (USA), N.A. based on the bank's failure to establish effective risk assessment processes prior to migrating significant

[15] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html
[16] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-159.html

information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner.[17] In October of 2020, the OCC assessed an $85M civil money penalty against USAA, Federal Savings Bank based on the bank's failure to implement and maintain an effective compliance risk management program and an effective information technology risk governance program.[18]

As evidenced by the enforcement actions discussed, the cost of this baselining project may be viewed by the cost of not doing the project. For example, the cost of regulatory penalty issued to the Bank in today's environment (*i.e.*, assuming a penalty- to-asset-size ratio holds steady) could range from $262k – $1.5M. Table 1 provides details to support this derived range:

**Table 1. Civil Money Penalty to Bank Asset Size**

| Bank | Penalty | Asset Size *(as of 12/31/2020)* | Penalty as % of Asset Size |
|---|---|---|---|
| Citibank, NA | $400M | $2,260B[19] | 0.0177% |
| JP Morgan Chase, NA | $250M | $3,400B[20] | 0.0074% |
| Capital One, N.A., and Capital One Bank (USA), N.A. | $80M | $421.6B[21] | 0.0190% |
| USAA Federal Savings Bank | $85M | $200.3B[22] | 0.0424% |

Burke & Herbert Bank assets as of September 30, 2021 totaled $3.56B[23]. Applying the low (0.0074%) and high (0.04234%) ends of the penalties as a percent of asset size yields the noted range of $262k to $1.5M.

[17] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html.
[18] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-135.html.
[19] https://www.citigroup.com/citi/investor/quarterly/2021/ar20_en.pdf, Page 3
[20] https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2020.pdf, Page 11
[21] https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_COF_2020.pdf, Page 17
[22] https://content.usaa.com/mcontent/static_assets/Media/report-to-members-2020.pdf?cacheid=2827458110_p&_ga=2.106829571.1090739150.1636053848-380228372.1634324640, Page 20
[23] https://www.burkeandherbertbank.com/wp-content/uploads/2021/10/Q3_2021_Financials.pdf, Page 2

Review of another institution highlights a different, but potential impact of ineffective risk management processes. In September of 2021, the OCC issued a Cease and Desist ("C&D") Order against MUFG Union Bank, N.A. based on the bank's unsafe or unsound practices regarding technology and operational risk management.[24] The day following the consent order, MUFG issued a press release noting U.S. Bancorp had announced it had entered into a definitive agreement to acquire MUFG Union Bank's core regional banking franchise. The article noted business synergies and spoke to US Bancorp's confidence that "…it can successfully remediate the issues applicable to MUFG Union Bank in connection with the transaction, and that the order will not restrict U.S. Bancorp's ability to operate and grow its business as planned."[25] Whether there was a cause and effect between the C&D and the acquisition announcement is unclear; however, the outcome reflects a risk other entities may experience if in a similar situation.

Review of fines incurred by one final institution, although not all-inclusive, provides insight into the potential lingering effects of alleged inadequate risk management practices. In September 2016, Wells Fargo Bank was ordered to pay $100M to the Consumer Financial Protection Bureau ("CFPB"), $50M to the City of Los Angeles and $35M to the OCC due to, per the CFPB, "the widespread illegal practice of secretly opening unauthorized deposit and credit card accounts."[26] Wells Fargo was also ordered to pay restitution to its customers, with one settlement reached in March of 2017, totaling $142M.[27] In February of 2020, Wells Fargo agreed to pay the Department of Justice $3B to resolve criminal and civil investigations into sales practices involving the opening of millions of accounts without customer authorization.[28]

[24] https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-100.html
[25] https://www.mufgamericas.com/who-we-are/news/u-s-bank-to-acquire-mufg-union-bank
[26] https://www.npr.org/sections/thetwo-way/2016/09/08/493130449/wells-fargo-to-pay-around-190-million-over-fake-accounts-that-sparked-bonuses
[27] https://en.wikipedia.org/wiki/Wells_Fargo_account_fraud_scandal
[28] https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices

Sharing these numbers is not meant to add to the cost estimates noted through the above penalty review, but more to punctuate the effects inadequate risk management practices can create.

The discussion of situations faced by other banks in the industry is meant to shine a light on potential consequences of ineffective risk management practices – from possible costly regulatory penalties, to potential acquisition of an institution, to a lengthy duration of regulator review, on-going imposition of fees and the likely continued impact to reputation.

The specific regulatory penalties provide a marker against which costs associated with the baselining project can be evaluated. The project, if implemented successfully, acts toward value preservation of the Bank. The estimates highlight potential dollars retained by the Bank with successful implementation of risk management practices and processes. Beyond the dollars noted, successful implementation will support potential reputational impacts of enforcement.

Review of project stages and personnel involvement supports evaluation of the expenses for this project. Table 2 provides a summary, noting in which stages the Board and team members may be involved. Cost estimates associated with each group follow the table.

**Table 2. Personnel Involvement by Project Stage**

| | **Build** | | | | **On-Going Management** | |
|---|---|---|---|---|---|---|
| | **Planning** | **Risk Inventory & Assessment** | **Risk Prioritization** | **Metrics & Reporting Build** | **Remediation & On-going Risk Management** | **Communication** |
| **Board of Directors** | | | | | | X |
| **Bank Management:** ***Project Leader*** | X | X | X | X | X | X |
| **Bank Management:** ***Current*** | | X | X | X | X | X |
| **Bank Management:** ***Incremental **** | X | X | X | X | X | X |

* Efforts may include a new full-time resource to support delivery. For conservatism, the full team member cost is aligned to the project (half-year salary for the Build and full year salary for On-Going Management)

**Board of Directors.** Costs associated with Board Member involvement relate to the Quarterly Risk Management Committee. Typical Board-level committees include four outside directors, with one acting as the Committee Chair. The compensation structure is $600 per meeting for the Chair and $500 per meeting for Members. With four quarterly meetings in a steady-state year, the resulting annual cost is $8,400, based on 1 outside director as Chair * 4 meetings / year * $600 / meeting plus 3 outside directors * 4 meetings / year * $500 / meeting. However, an existing Board-level committee (*e.g.,* Bank Secrecy Act Committee) could assume coverage of both current scope and the additional risk topics. If this were to occur, the cost of Board of Director involvement is neutral to current state.

Training may also be of value for the Board, at a minimum for Committee members. Courses are offered through the American Bankers Association ("ABA") and are free of charge given the Bank's membership level. While no cost would be incurred to complete courses such as Board and Senior Management Oversight and Introduction to Enterprise Risk Management[29], Board member time would be needed. Further training options could also be explored over time.

**Project Leader.** While in reality there is not an additional cost for the Project Leader's time on this project, one could argue there is an opportunity cost due to focus on this project rather than other potential Bank priorities. As such, these opportunity costs are estimated below:

- *Planning*. This project stage is expected to last 4-6 weeks, estimated at 25% of resource capacity. Assuming 40 effective (non-administrative) work hours in a week, the resulting hours estimate during this stage is 40 hours * 5 weeks (the mid-point of the range) * 0.25, or 50 hours.

[29] https://www.aba.com/training-events/online-training/certificate-in-risk-management-frameworks

- *Risk Inventory & Assessment*. This project stage is also anticipated to run 4-6 weeks. The project leader is estimated to spend a targeted 15% of capacity. Similar effective work hours leads to 40 hours * 5 weeks * 0.15 or 30 hours.
- *Risk Prioritization*. This project stage is estimated to last 3 weeks and will include analysis, discussion and read-out to management. The project leader may spend 30% of their capacity in this stage, or 40 hours * 3 weeks * 0.30 or 36 hours.
- *Metrics & Reporting Build*. The Project leader will guide general information needs but actual reporting efforts will be completed by risk owners. The role in this stage is one of inquiry and response and meeting facilitation. The project leader may spend 5% of their capacity during these four weeks, or 40 hours * 4 weeks * 5%, or 8 hours.
- *Remediation & On-going Risk Management.* In this on-going stage, the project leader will facilitate tracking and enhancement efforts, using an estimated 2% of capacity; some weeks will be more, others will be less. The estimate leads to 40 hours * 44 weeks (52 weeks, less 6 weeks of vacation and 2 weeks of holidays) * 2%, or ~36 hours. As a reasonability test, these 36 hours lead to likely 9 hours per quarter.
- *Communication.* Finally, the project leader will be responsible for facilitating quarterly Board-level meetings. An estimate of 8-12 hours in discussion material development yields 10 hours (the mid-point) * 4 quarters or 40 hours / year on-going.

In summary, while not an actual spend, the project leader cost estimate includes the sum of the hours in the building stages (Planning through Metrics & Reporting Build), or 124 hours and the on-going management costs (Remediation & On-going Risk Management and Communication) or 76 hours. Assuming an hourly rate of $120, one-time build costs are estimated at approximately $15k; on-going at ~$9.2k per year.

**Bank Team Members.** Similar to the project leader, there is not likely additional cost tied to team member time as each is already managing their risks. However, one could argue a similar opportunity cost due to focus spent on this project rather than other Bank priorities. An important starting point for this estimate is understanding the number of team members who may be involved. Using the Bank's Key Controls ownership as an analog suggests 19 team members may be involved in this project and on-going efforts. Costs are estimated below:

- *Risk Inventory & Assessment*. This project stage is anticipated to require two meetings, at one to two hours each with the complement of risk owners. While more than one risk owner may participate in a meeting, each of the total 19 will participate. The resulting hours in this stage are 19 * 3 (mid-point of estimate) or 57 hours.
- *Risk Prioritization*. This project stage will likely engage the complement of risk owners in discussion to review the assessment results. Review of materials and meeting participation is estimated at 2 hours for each team member, or 38 hours.
- *Metrics & Reporting Build*. Risk owners will likely be most heavily engaged in this stage, but should also be able to leverage existing reporting. Some additional engagement time needs to be considered for incremental metrics build. This effort is estimated at 2 days per team member; that is, 16 hours * 19 or 304 hours.
- *Remediation & On-going Risk Management.* Remediation efforts will largely be business as usual and not require incremental time. However, on-going meeting participation and communication may be new. Management meetings are expected to occur quarterly, with delivery of metrics and meeting participation estimated to be 8 and 1 hour, respectively, resulting in 9 hours * 19 team members * 4 quarters or 684 hours. Other forums, if added, would add time but are not considered here.

- *Communication.*  These costs are mainly captured in On-going Risk Management; however, some leadership time will be involved in quarterly Board-level meetings. This estimate is similar to the Board Committee in that it may be cost neutral if Management expands an existing committee purpose.  If not, 3 Senior Executives would spend 2 hours each quarter in these discussions or 24 hours / year.

In summary, while not an actual spend, the project team cost estimate includes the sum of the hours in the building stages (Planning through Metrics & Reporting Build) or 399 hours and the on-going management costs (Remediation & On-going Risk Management and Communication) or 708 hours. Assuming an hourly rate of $150, one-time build costs are estimated at approximately $60k; on-going at ~$106k per year.

Further, as noted earlier, for conservatism, project cost estimates suggest a new full-time Enterprise Risk Manager to support the project leader and team members in delivery.  Based on Bank Human Resources input, the annual salary for this dedicated role is likely to be $90k.  With the Build element of the project expected to last nearly six months, half of the annual salary is aligned to this effort; the full annual salary is aligned to On-Going Management efforts.  See Appendix B for a job description, which includes reporting structure of the role.

Finally, the program may benefit from team member participation in a risk management conference to enhance knowledge and potentially influence framework evolution.  The ABA has not yet released conference costs, but using prior years as an analog suggests an estimate of $1,500 for participation plus travel at $2,500 (internal travel budget heuristic), or $4,000 per person.  Sending two team members each year may help with information sharing and program support.  As such, $8,000 is budgeted in the Build and on-going management stages.

Overall costs are estimated at $128k to build and $222k to maintain the program. These results are noted below in Table 3.

**Table 3. Overall Project Cost Estimates**

| | Build, one-time hours and dollars | | | On-Going Management, Annual hours and dollars | |
|---|---|---|---|---|---|
| | **Total hours** | **Rate / hour** | **Total** | **Total Hours** | **Total** |
| **Board of Directors** | | | | *Set Director Fees* | $8,400 |
| **Bank Management:** ***Project Leader*** | 124 | $120 | $14,880 | 76 | $9,120 |
| **Bank Management:** ***Current*** | 399 | $150 | $59,850 | 708 | $106,200 |
| **Bank Management:** ***Incremental **** | | | $45,000 | *Full time resource* | $90,000 |
| **Training (Overall)** | | | $8,000 | | $8,000 |
| Total | | | **$127,730** | | **$221,720** |

* Efforts may include a new full-time resource to support delivery. For conservatism, the full team member cost is aligned to the project (half-year salary for the Build and full year salary for On-Going Management)

### *Assumption Sensitivity Review*

As with any estimation effort, the quality of the result relies on the quality of the inputs. While the discussion above aims to be deliberate and clear in the estimates, there are some costs that may in reality be different than the estimates.

Key drivers of the success of this initiative include Bank team member engagement in the process and the ability to prioritize this work relative to other activity. This latter point becomes important to the cost impacts; with limited focus or limited availability, the time to deliver may extend. This extension could increase project leader time on the project and build, increasing the opportunity cost associated with delivery.

In a best case scenario, business lines will own their risk identification role and have the ability to leverage existing information for their metrics and reporting needs. In addition, they will be able to effectively assess overlapping effects of their risks on other areas of the Bank and will be in a position to engage and assess the impact of other areas' risks on their own. The full team will be engaged from the start in the baseline work and input will help to advance the program within the organization. This best case may or may not reduce the costs associated with Board, business line or project leader time, but, as discussed in the next section (Non-Financial Impact) could have a broader positive outcome on how the organization perceives risk management, *i.e.,* culture. The one real cost that could be affected by the build is in the hiring of an additional resource to support facilitation of the risk management process at the Bank. The full resource cost of $90k is currently allocated to this work on an annual basis; if there is quick and robust business line adoption and ownership, the need for full time focus may reduce; however, the on-going facilitation would still be needed. Estimated benefit could be up to 50% of this individual's time. As the salary would not change, the time gained could be applied to other Bank priorities.

In a worst case scenario, team member alignment with the effort is likely not achieved. As such, the ability to identify and prioritize risks to enable management of key risks becomes the challenge. In this case, there are likely extensive discussions with no real benefit or outcome. In addition, visibility to the integrated impacts of risk is not understood. Further, the culture of risk management is negatively impacted, which could have longer term impacts on the ability to launch and deliver risk management efforts in the future. In this situation, the work of the project leader and the team is at best a sunk cost, but given the focus without delivery, it is a negative to the business since the team was unable to focus on other potentially more beneficial efforts during this time. The situation would be considered an "epic fail" of the rollout.

In a most likely scenario, some business lines will quickly adopt the risk practices (*e.g.*, credit, financial, compliance) while others may need time and education. In this case, leaning on early adopters to demonstrate the benefits of the rollout will likely support a positive outcome.

The range from worst to best case scenario in delivery relies on strong communication. This communication is needed between the project leader and participants and with key leaders in the organization. Some discussions may need to be one-on-one, while others may be broader messaging, aiming to build understanding across the group. If and when additional leadership engagement may be beneficial to delivery, the project leader must escalate; however, it is important to balance how often this escalation occurs to build buy-in from the team.

### *Investment Go / No-Go Discussion*

Ultimately, the decision to move forward with the project to baseline an integrated risk management program at the Bank comes down to perceived benefit relative to estimated cost. The benefits are not likely to be financially-driven totals that would accrue to the bottom line of the organization. Rather, effective risk management practices will be more aligned to value preservation of the organization. Applying both an internal and an external lens to the decision aids in the final go recommendation to move forward with the project.

From an internal perspective, strong risk management practices support growth goals of the organization. Understanding areas of risk and addressing them will enable not only current safe and sound business operations but also future operations. As noted earlier, growth may come from additional customers, through offering new products and services and more broadly, through potential acquisition. Clarity regarding performance will allow the Bank to address those needs as-needed and on an on-going basis. Further, strong risk management processes may also support acquisition decisions, as the Bank may be better able to evaluate risks inherent in the target institution.

This understanding not only supports growth, but it also protects the Bank's reputation. Said simply, "Reputation is one of the most important assets for companies today. Companies with a strong reputation perform better, attract qualified employees and increase their overall success."[30] The baseline and on-going delivery of the risk management framework will protect the Bank's storied history and its reputation, ensuring decisions are made with an understanding of the potential impact across risk categories, including this important somewhat intangible area.

Finally, while not necessarily immediately quantifiable, there is a potential outcome where, through conversation and understanding of risk practices across the organization, the Bank may identify areas where it may in fact take on more risk, where sufficiently financially justified. Learning from and applying process across various business lines may lead to increased financial performance.

From an external perspective, the headline enforcement actions noted earlier paint the picture of incremental cost avoidance. With a focus on a strong risk management framework now, the Bank will be in a position to own its narrative regarding its approach. On-going opportunities for enhancement can be identified and furthered, but the baseline allows the Bank to build its approach.

Moreover, other external review supports the go recommendation for the baseline effort. The pace of risk events is increasing. The recent rise in ransomware attacks demonstrates the susceptibility of financial institutions and the potential costs incurred. For example, one headline raises attention to the increasing dominance of ransomware attacks, noting, "Banking industry

[30] https://prevency.com/en/what-is-reputation-risk-management/

sees 1318% increase in ransomware attacks in 2021."[31] Further, a recent report from the Financial Crimes Enforcement Agency ("FinCEN") notes an increase in the number of Suspicious Activity Reports ("SAR") and the associated dollar value of the suspicious activity – from 487 total SARs in 2020 to 635 SARs in the first half of 2021 and from a total 2020 value of $416M to $590M in the first half of the 2021.[32]

In addition, regulatory change in support of new, emerging areas of risk is on the horizon. For example, regulators continue to discuss climate change risk and have recently noted plans to release a high-level framework for regulatory guidance as early as the end of 2021.[33] While actual regulation would follow in time, this focus demonstrates the changing operating environment and risk management expectations. Connected to but separate from climate change risk is an additional emerging area of regulatory focus – Environment Social and Governance ("ESG") issues. These issues will not necessarily be unique from other areas of the Bank, but rather may connect to Bank policies and decisions (*e.g.,* potential incorporation into lending and investment decisions).[34] Regulatory efforts in the ESG space are in the early stages, but the conversations note the pace of change and the evolving areas of risk management facing the industry. Building the framework today allows for advancement and enhancement if or when these changes come to be.

In summary, the go recommendation supports the Bank's growth strategy. It mitigates, although does not fully eliminate, risks related to the environment in which the Bank operates. And, it sets the stage for future enhancements for on-going safe and sound operation.

[31] www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021
[32] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf, Page 1.
[33] https://bankingjournal.aba.com/2021/11/acting-occ-chief-addresses-climate-change-risk-regulation/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20211109
[34] https://www.thomsonreuters.com/en-us/posts/news-and-media/esg-regulations-financial-firms/

## Non-Financial Impact

### *Potential Hurdles*

Implementing organizational change can take time and may be met with resistance. While management of risk will not be new to the organization, there are a few hurdles that will need to be considered through this effort. These may be summarized as resistance to oversight, an inability to resource and potential knowledge gaps. Each is further detailed below.

As discussed earlier, risks are currently managed (mainly) in siloes across the Bank. Experts identify, assess and action their risks as needed, be they in credit metrics, financial measures or compliance reviews. Introducing an oversight function may be perceived as a "take-over" of risk management practices for the Bank overall. This change, while not the intent, may be further perceived as reducing the expertise in risk management routines, thus diminishing the effectiveness of practices. Finally, oversight could create a risk management ownership risk, if perception of centralization is that practices are forfeit to the oversight function.

An additional hurdle is the resourcing that may be perceived as necessary to support the build and on-going delivery of the risk management framework. As a smaller institution, with resources and expertise tapped to support business as usual as well as enhancement efforts, another project may be seen as a challenge to deliver. While there may be positive intentions, human nature may kick-in, with the additional reporting, discussion and on-going management being seen less as something most are currently doing and more as something new to add to an already full plate of expectations.

A third hurdle may be viewed less from a willingness lens and more from a skill lens. That is, some team members may not have the experience, knowledge or understanding to fully identify, evaluate and prioritize risks and utilize metrics to inform risk posture.

### *Approach to Overcoming Hurdles*

Understanding potential obstacles is often the first step to addressing them. An important element in overcoming the potential hurdles noted above is communication; it is core to aligning team members toward a target objective. Open dialogue can play an important role, both in overcoming the obstacles and in building a strong risk management baseline.

For example, in response to the oversight concern, communication can be clear and direct, noting the interaction is not about micro-managing a particular area of risk for the Bank. Rather, it is about elevating the conversation about key risks and enabling awareness of potential cross-organization impacts of individual risks. Making these statements and demonstrating through action may be two different, yet equally important steps. Through communication, the project leader can engage risk managers in the problem solving process, leveraging their expertise to build a stronger program overall. Those leaders that have metrics in place for key risks have, either explicitly or implicitly, applied a prioritization heuristic for why managing the risk is important. Understanding these heuristics can inform the broader program, thus, engaging key players in the solution.

Further, this engagement in the solution can also support concerns about resourcing "yet one more project." With inclusion in the problem solving, team members may see that they are not only applying work they are, in many cases, already doing for the Bank, but also using it to support broader risk management goals. Not all of the activities to baseline the risk management framework are currently in place at the Bank; there will be some incremental work as well (*e.g.*, potential additional evaluation and reporting efforts); however, providing the context, sharing the roadmap for additional elements expected over time (*e.g.,* inclusion of risk appetite, risk tolerance) and engaging in the build may support early buy-in and on-going adoption.

Finally, as knowledge increases, so does confidence in delivery. Risk management training may be beneficial for some or many of the Bank's team members. This training may be specific to Bank needs or it may relate to broader risk management needs. As program planning and discussions unfold, training needs will become clearer. Once understood, decisions can be made for build-or-buy training options; that is, building through the Bank's in-house university or staffing through external resources. As noted earlier, the financial impact of the project includes conference participation for two team members per year; in addition, the ABA training curriculum offers risk management training, which may be a foundation upon which to build.

Overall, communicating to understand what is in place today and what may be needed going forward, engaging team members in problem solving and making clear the unique roles that team members play can support the delivery of this baselining project.

***Measuring Non-Financial Impacts***

Metrics can help Bank management understand the impact of the risk management baselining efforts. Measures will focus primarily on internal parameters related to culture as it is critical to successful and sustained implementation. Learning from current risk management practices as noted in the Project Rationale discussion, these elements include team member awareness of the importance of managing risks and escalating issues; adoption of common vernacular; and use of objective measures (*e.g.,* key risk indicators) in decision-making.

Culture is often supported through understanding expectations. Creating awareness and establishing a baseline understanding of performance relative to those expectations is a first step. Routinely assessing that performance will help evaluate the progress of the framework rollout, adoption and consequently the culture of risk management.

Further, a common language, or vernacular, can support culture. It can enable clear communication and understanding, reducing the potential for team members to hear the same words but interpret them differently.

Finally, an outcome reflective of a culture of risk management is the utilization of metrics in decisions where risks need to be considered. Across many areas, these metrics are already in use. For example, credit decisions leverage underwriting parameters to address risk factors. An increased use of metrics, both within individual areas and across a broader spectrum (*e.g.*, end-to-end processes) may support further grounded, informed outcomes.

***Detailed Non-Financial Impact Analysis***

A strong, positive culture can create benefit for team members, the organization and the community of customers as a whole. Culture is the expected way of interacting both internally and externally. It includes operating norms as well as the processes and shared experiences that consistently underpin how work is done and how team members engage to accomplish objectives. Culture is supported by the elements noted above, including awareness of expectations, utilization of common vernacular and use of metrics to guide decisions.

Awareness aims to address what may appear to be a simple question, but in actuality can be more complex, "Do team members understand expectations of them regarding management of risk?" Culture and consistent operating norms create clarity for team members as they support that understanding of expectations. These expectations include their roles, the roles of others and the connections between and across them. Awareness creates a baseline from which open dialogue can occur, which may support enhanced teamwork, generation of new ideas and, if needed, delivery of meaningful change. Further, this awareness can lead to increased job satisfaction as alignment of objectives may be better enabled. Awareness does not mean interactions will be easy, but it does mean there is a common base from which to work and aim to build positive outcomes through cohesion in delivery.

The organization also benefits from a culture where expectations are understood. With team member job satisfaction, there is likely less turnover in the organization and less cost associated with hiring. Spend can target skill building, which becomes more focused on development and advancement of team members rather than replacement. A tenured employee base can contribute to on-going delivery and use of institutional knowledge in identification of issue areas and opportunities for improvement, although it is important to enable the space to have open dialogue for raising potential issues. Awareness of expectations can also identify knowledge or skill set gaps for which the organization may need to procure talent, potentially through hiring or use of outside support. If the organization chooses to use outside support, the expectations can form the basis of service level agreements and review processes with vendors. Understanding needs will help inform this decision in a disciplined, structured manner.

Awareness also supports the Bank's customer experience. Clear expectations and disciplined process execution (*e.g.*, new product and services rollout) can translate to better delivery, creating more positive interactions, less customer confusion or frustration and increased retention and depth of relationships in the long-term.

Long-term profitability is supported through team member awareness of risk management expectations. Awareness enables dialogue, which allows for issue discussion and resolution, more effective on-going delivery of processes and continued customer retention.

To measure the level of awareness of risk management expectations, the Bank can consider adding a question(s) to its employee questionnaire. The first response set can form the baseline to assist in prioritizing where early focus might be best applied. On-going responses can serve to form trends, creating a living agenda. From a customer perspective, the Bank can utilize its customer complaints information as well as social media commentary to assess if any particular topics or experiences rise to the level risk management attention, particularly topics that may be associated with reputation risk. Finally, the Bank can consider other voice of the customer initiatives, similar to the internal employee questionnaire; example questions might cover customer confidence in the Bank's safeguarding of data and meeting customer needs.

Common vernacular can also support a strong, positive culture; it aims to understand the question, "Do team members understand terms applied in risk management?" While open dialogue is important, tied to that dialogue is shared understanding. It leads to team members being on the same page and reducing the potential for them to hear the same words but interpret them differently. For example, terms such as exception, violation, issue, finding and opportunity are all words that may be used by first, second and third lines of defense. However, an exception could be procedural, a violation regulatory, and an opportunity a best practice. Without common understanding, managers may be left to their own interpretation, with resulting action planning potentially misaligned with the identified level of risk.

If team members are able to effectively communicate with common language, the organization also benefits. Assumptions can be minimized, which can lead to less re-work and greater effectiveness.

Similar to awareness, common vernacular may also benefit customers as team members understand what is being asked. It can translate to better delivery and creation of more positive, less confusing interactions, which over time supports enhanced retention and relationship depth.

Long-term profitability also benefits from common language. When an organization is communicating clearly, it is likely more well-managed than not. When it is well-managed, its effectiveness, and often efficiency, improve, driving less costs associated with rework, remediation or retooling. Further, additional capacity is created in the system and can be applied to support other prioritized objectives; prioritization which is often driven by financial impact.

Measuring the benefit of common vernacular can occur through use of the questionnaire process noted in the above awareness discussion. The Bank can consider adding a question(s) to its employee questionnaire to baseline and assess the on-going use and understanding of terminology in risk management-related communications.

Perhaps the largest opportunity to impact the culture of risk management is the use of Key Risk Indicators ("KRIs") in each risk area and across the Bank as a whole. In fact, this opportunity is considered to be so important that there is a dedicated metrics stage noted in the risk management baselining project plan. KRIs help to answer the question, "How do leaders and team members make decisions related to risk management?"

Metrics support fact-based decision-making, where rationale is grounded in objective data, complemented by interpretation and perspective. Use of KRIs does not preclude interpretation and qualitative judgement; rather, it supports review of risk levels and potential impacts of failure events. As mentioned earlier, several areas of the Bank have metrics in place; however, leveraging an integrated discussion creates clarity into potential intersections of risk (*e.g.,* error rates on disclosure provision may be low from an operational view, but high from a compliance standpoint); understanding these intersections supports a well-managed organization.

Use of metrics reinforces process performance and opportunities for team members in delivery. They are able to see clearly the relationship among work, results and potential issues. They may be empowered to utilize this information to support identification of improvement needs or opportunities for efficiency and the subsequent impact of remediation activities.

The organization, as noted above, benefits with use of metrics due to grounded, objective data enabling decision-making needs. In addition, through this objective data, there are early warning signals to potential areas of concern. Further, there is empowerment of team members for identification and remediation activities.

Customer benefit is similar to the impact of awareness and common vernacular. Metrics enable a well-managed organization, which supports strong execution of delivery processes, less customer confusion and greater likelihood of a positive customer experience. Well-managed likely also leads to enhanced customer retention and relationship depth.

Further, use of KRIs supports long-term profitability as there is an ability to not only baseline a metric, but also to learn from performance and continue to enhance and advance the measurements over time. In some cases, KRIs may be tightened, while others may be relaxed based on the business environment and risk tolerance. These changes should be informed by data, with an ability to continue to measure and adjust, if / as needed. Changes should be carefully reviewed with a focus on calibrating risk and reward informing decisions. This work does not happen overnight; it requires a baseline and a culture supportive of on-going learning.

Measuring utility of KRIs is likely a qualitative endeavor, with a review of how metrics are used, how they evolve and how they inform and limit potential risk events from occurring. More than evaluating the number of KRIs, the quality of the KRIs should be the aim. Questions such as “Did the Bank stay ahead of risk events?” and “Did the Bank respond in a timely and complete manner if a risk occurred?” are just two discussion points that could occur with Bank leadership. Maintaining an on-going dialogue of these and other utility questions will support clarity into the benefit of current KRIs and the potential needed evolution.

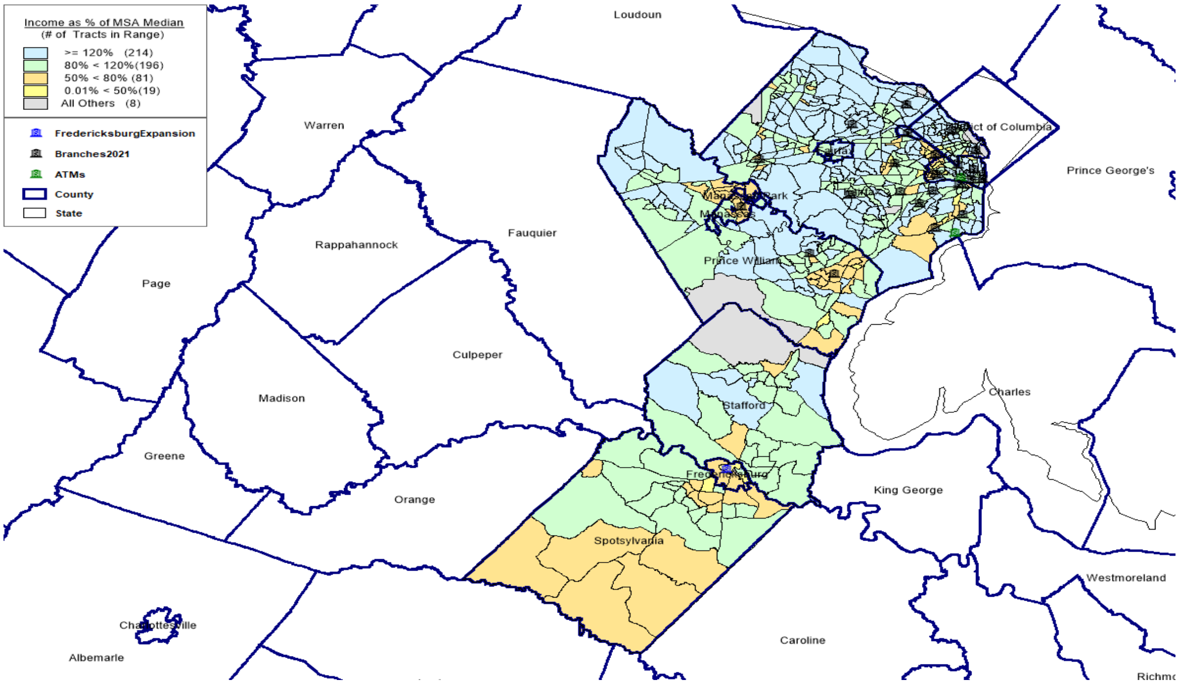
## Conclusion

In summary, creation of an integrated enterprise risk management program, enabled through implementation of the risk management baselining project is beneficial to the Bank in both the near- and long-term. Developing processes today sets the Bank on a journey of understanding its key risks and leveraging practices to address them in a holistic way. It creates the foundation on which future growth (*e.g.*, products and services, geography and organization expansion) can be supported while also preserving value of the organization. It enables the Bank to adapt to the often fast changing external risk landscape. Further, in an environment where regulatory scrutiny continues to increase, it allows the Bank to own its narrative regarding how it manages risk across the organization in a disciplined and coordinated manner. Finally, it likely leads to enhanced long-term customer impact, as stronger operational execution, less fraud and new products that are subject to rigorous review processes should ultimately lead to customer benefit, with increased likelihood of retention and depth of relationship. Taken together, the strength of the Bank's risk management program will contribute to its business success as well as on-going positive reputation in the community.

The build will take time and energy from Bank team members, but there is a basis upon which to build as several leaders have processes in place. Leveraging communication, engagement and effective challenge across the organization will help in initial stand-up as well as on-going sustainability and advancement of the program. Metrics and on-going communication will help frame future priorities and program evolution to support the Bank's strategic objectives and a well-managed agenda. Altogether, project implementation mitigates, although it does not fully eliminate, risks related to the environment in which the Bank operates. As such, it sets the stage for future enhancements and continued safe and sound operation.

## Appendix A: Burke & Herbert Bank Geography

Source: CRA Wiz



## Appendix B: Functional Job Description Enterprise Risk Management Manager

### Summary/Objective

Under direction of the Chief Compliance Officer, the Enterprise Risk Management ("ERM") Manager will support the organization regarding the build and on-going delivery of the Bank's ERM management program. Responsibilities include supporting the identification of risks throughout the organization, the development of reporting and monitoring formats and the enhancement of methodologies for the assessment of risks throughout the organization. The role will require collaboration with various lines of business and documentation of risk discussions. Further, the individual will review results and conduct analysis to support prioritization of key risks. The position requires great attention to detail with excellent oral and written communication and analytical skills.

### Essential Functions

1. Supports the Chief Compliance Officer by developing Enterprise Risk Management ("ERM") tools, practices and policies to analyze and report enterprise risks
2. Engages directly with business lines in inquiry and discussion to understand specific risks and connectivity across the organization's risks overall
3. Applies analytical skillset to establish the set of prioritized key risks to be managed through the ERM process at the Bank
4. Utilizes honed communication skills to review results with business lines and confirm reasonableness of prioritization conclusions
5. Provides guidance to business lines regarding Management and Board-level reporting expectations for key risks
6. Acts as liaison for integration and status reporting information to Management and the Board of Directors
7. Facilitates risk remediation and acceptance tracking and supports on-going development of tools and program enhancements
8. Performs other duties as assigned

### Skills/Abilities

1. Excellent organizational skills and strong attention to detail
2. Strong critical thinking and analytical skills, applied at big picture and detailed levels
3. Strong initiative, with an ability to drive work and adapt to change
4. Strong interpersonal, written, verbal communication, inquiry and listening skills
5. Ability to work both independently and in a team environment
6. Ability to complete duties with discretion and confidentiality reflecting the sensitive nature of the work
7. Proficient with Microsoft Office applications, specifically Excel and PowerPoint

### Education and Experience

1. Bachelor's Degree required
2. Minimum five years' experience in a similar risk management facilitation or delivery role
3. Financial services industry experience preferred
4. Certified Enterprise Risk Professional (CERP) or similar preferred

**Bibliography**


- About Us, *Burke and Herbert Bank corporate website,* viewed 10 August 2021, <https://www.burkeandherbertbank.com/about/>.

- Phaneuf, A 2021, *The disruptive trends & companies transforming digital banking services in 2021*, viewed 25 August 2021, <https://www.insiderintelligence.com/insights/digital-banking-trends/>

- Williams, Julia, *Burke & Herbert Celebrates 150 Years A living legacy of Commitment and Service.* Richmond: The Dietz Press, Inc., 2002.

- Burke & Herbert Bank. (2020) Town Hall 1_21_2020 Final. Unpublished internal company document

- Burke & Herbert Bank 2021, *Q2_2021_Financials*, viewed 10 August 2021, <https://www.burkeandherbertbank.com/wp-content/uploads/2021/07/Q2_2021_Financials.pdf>

- FDIC Deposit Market Share Reports – Summary of Deposits 2021, *FDIC* website, viewed 10 August 2021, < https://www7.fdic.gov/sod/>

- Kleimann, J 2021, *Here are the top 15 mortgage lenders of 2020,* viewed 10 August 2021, < https://www.housingwire.com/articles/here-are-the-top-15-mortgage-lenders-of-2020/>

- Proctor, C 2021. *Largest Home Mortgage Lenders in Greater D.C.*, viewed 10 August 2021, <https://www.bizjournals.com/washington/subscriber-only/2020/04/10/largest-home-mortgage-lenders-in.html>

- Office of the Comptroller of the Currency 2021, *Federal Register*, viewed 10 September 2021, <https://www.occ.gov/news-issuances/federal-register/2014/79fr54518.pdf>

- nContracts 2021, Kumbaya! Bringing Together Risk, Compliance & Other Business Units, viewed 26 August 2021, < https://www.ncontracts.com/risk-and-compliance-together.pdf>

- Office of the Comptroller of the Currency 2021, *News Release 2020-132*, viewed 4 November 2021, <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html>

- Office of the Comptroller of the Currency 2021, *News Release 2020-159*, viewed 4 November 2021, <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-159.html>

- Office of the Comptroller of the Currency 2021, *News Release 2020-101*, viewed 4 November 2021, <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html>

- Office of the Comptroller of the Currency 2021, *News Release 2020-135*, viewed 4 November 2021, <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-135.html>

- Citigroup 2021, *ar20_en*, viewed 4 November 2021, <https://www.citigroup.com/citi/investor/quarterly/2021/ar20_en.pdf>

- JP Morgan Chase Bank 2021, *annualreport-2020*, viewed 4 November 2021, <https://www.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/investor-relations/documents/annualreport-2020.pdf>

- Capital One Financial Corporation 2021, *NYSE_COF_2020*, viewed 4 November 2021 <https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_COF_2020.pdf >

- USAA Federal Savings Bank 2021, *2020 USAA Report to Member PDF*, viewed 4 November 2021, <https://content.usaa.com/mcontent/static_assets/Media/report-to-members-2020.pdf?cacheid=2827458110_p&_ga=2.106829571.1090739150.1636053848-380228372.1634324640>

- Burke & Herbert Bank 2021, *Q3_2021_Financials*, viewed 4 November 2021, <https://www.burkeandherbertbank.com/wp-content/uploads/2021/10/Q3_2021_Financials.pdf>

- Office of the Comptroller of the Currency 2021, *News Release 2021-100*, viewed 4 November 2021, <https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-100.html>

- MUFG Americas, *U.S. Bank to Acquire MUFG Union Bank,* viewed 4 November, <https://www.mufgamericas.com/who-we-are/news/u-s-bank-to-acquire-mufg-union-bank>

- Chappell, B, 2016, *Wells Fargo Fined $185 Million Over Creation Of Fake Accounts For Bonuses*, viewed 4 November 2021, <https://www.npr.org/sections/thetwo-way/2016/09/08/493130449/wells-fargo-to-pay-around-190-million-over-fake-accounts-that-sparked-bonuses>

- *Wells Fargo account fraud scandal* 2021, viewed 4 November 2021, <https://en.wikipedia.org/wiki/Wells_Fargo_account_fraud_scandal>

- The United States Department of Justice, *Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts without Customer Authorization*, viewed 4 November 2021, <https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices>

- American Bankers Association, *Certificate in Risk Management Frameworks*, viewed 15 December 2021, < https://www.aba.com/training-events/online-training/certificate-in-risk-management-frameworks>

- Prevancy, *What Is reputation risk management?*, viewed 12 November 2021, <https://prevency.com/en/what-is-reputation-risk-management/>

- Henriquez, M 2021, *Banking industry sees 1318% increase in ransomware attacks in 2021*, viewed 10 November 2021, <www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021>

- FinCEN 2021, *Financial Trend Analysis.pdf*, viewed 12 November 2021, <https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf>

- ABA Banking Journal, *Acting OCC Chief Addresses Climate Change Risk Regulation*, viewed 12 November 2021, <https://bankingjournal.aba.com/2021/11/acting-occ-chief-addresses-climate-change-risk-regulation/?utm_source=eloqua&utm_medium=email&utm_campaign=newsbytes&utm_content=NEWSBYTES-20211109>

- Thomson Reuters, *US financial firms should prepare for ESG regulations, with sustainability a key focus*, viewed 12 November 2021, <https://www.thomsonreuters.com/en-us/posts/news-and-media/esg-regulations-financial-firms/>