Apple Financial Holdings, Inc.

Risk Management Framework Policy

November 17, 2021

Contents

I. POLICY PURPOSE STATEMENT AND SCOPE 4

II. DEFINITIONS 4

III. KEY POLICY COMPONENTS 6
1. Executive Summary 6
2. Objectives 6
3. Key Components of Policy 6
1) Core Risk Management Principles 7
2) Risk Identification Process 9
3) Risk Appetite 9
4) Risk Limits, Risk Indicators and Metrics 10
5) Key Reviews and Risk Assessments 12
6) Referential Data and Bank-wide Taxonomies 14
4. Escalation Procedures 16

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE 17

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS 17

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW 18

VII. EXCEPTIONS TO THE POLICY 18

VIII. RETIREMENT OF POLICIES 18

IX. ROLES AND RESPONSIBILITIES 18

X. RECORD RETENTION 20

XI. QUESTIONS AND CONTACT INFORMATION 20

XII. LIST OF REFERENCE DOCUMENTS 20

XIII. REVISION HISTORY 20

POLICY NAME: Risk Management Framework Policy

REVIEW AND TRACKING CHART

Effective Date*:	November 17, 2021
Version Number:	4.3
Policy Level:	Policy Level 1
Corresponding Board Review Frequency:	Annual (Every 12 Months)
Board or Designated Board Committee:	Board Risk Committee (BRC)
Last Board Review Date*:	November 17, 2021
Next Board Review Date*:	November 2022
Designated Management Committee:	Management Risk Committee (MRC)
Last Management Review Date*:	November 4, 2021
Next Management Review Date*:	November 2022
Policy Owner:	Richard Leite, SVP, Risk Management

I. POLICY PURPOSE STATEMENT AND SCOPE

This Risk Management Framework ("RMF") formalizes a consistent Bank-wide approach to risk management and ensures it is adhered to across the organization at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank"), to the extent applicable to such entity, in accordance with applicable state and federal statutes, rules and regulations.

All ABS employees and third party resources engaged by the Bank must comply with the terms of this Policy to the degree applicable to them.

II. DEFINITIONS

- **Annual or Annually: Every twelve (12) months.**

- **Control Form:** The form to be submitted to the PPA (defined in this section) in connection with revised Policies, Standards, Procedures, or Manuals. The Control Form is available on AppleNet.

- **Immaterial Change:** A change that does not alter the substance of the Policy in any way, but rather is a change only to grammar, formatting, template, typos, and the like.

- **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for this Policy. The attorney does initial and ongoing reviews of the Policy and serves in an advisory capacity.

- **Material Change:** A change that alters the substance of the Policy in any way or how it is applied, such as a change to a definition, phrase, vendor name, threshold, or anything beyond an Immaterial Change as defined above.

- **Policy Level 1**: A Regular Board Review Cycle level for a Policy, designated by Risk Management in consultation with Legal. Level 1 Policies require Annual approval by the Board or a Designated Board Committee.

- **Policy Owner:** The person responsible for managing and tracking a Policy. This includes initiating the review of the relevant Policy and recommending updates to the Policy, to the extent needed. Policy Owners are responsible for obtaining the appropriate level of approval and providing the approved documents to the PPA (as defined in this section) for upload to AppleNet. Additionally, the Policy Owner is responsible for presenting revisions and Policy exception requests for consideration.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Policy reviews, obtains the updated versions of Policies, and ensures that they are uploaded to AppleNet. The PPA shall

review Policies and advise the Policy Owner if procedures have been errantly included in the Policy, and the Policy Owner shall revise accordingly. The PPA will also provide guidance regarding the use of the PPGP (as defined in this section) to Bank Personnel.

- **Policy and Procedures Governance Policy (PPGP):** The PPGP establishes a standardized and consistent approach to the creation, review, approval and maintenance of Policies, Standards, Procedures, and Manuals across the Bank.

- **Policy, Standards, Procedures, and Manual Index:** An index, maintained by the PPA, which sets out the Policy, Standards, Procedures, or Manual name, Owner, regularly scheduled review dates, Regular Board Review Cycle (to the extent applicable), Designated Management Committee, and Designated Board Committee (to the extent applicable). The index is available on AppleNet.

- **Regular Board Review Cycle:** The required periodic Board or Designated Board Committee approval process for a Policy, the frequency of which is determined by the designation of a Policy as a Level 1, Level 2, or Level 3 Policy.

- **GRC Tool:** the Governance Risk and Compliance (GRC) tool is a commercial application, accessible via a web browser, that allows the Bank to (i) capture issues and incidents from across the organization, (ii) perform risk control self-assessments (RCSA's) and controls testing in a less manual fashion, and (iii) track issue and action plan ownership and remediation in a centralized manner. The tool leverages common libraries, taxonomies and tooling which can be leveraged by other second-line of defense and third-line of defense functions for performing similar issue and incident capture, risk assessments, risk analysis and reporting.

- **Risk Type:** Broad categories of risks, grouping similar risk exposures into an overall class (e.g., market risk, credit risk, operational risk, reputational risk, etc.).

- **Risk Capacity:** Risk capacity refers to the maximum amount of risk that the Bank can take and continue to operate within regulatory well-capitalized minimums.

- **Risk Appetite:** Risk appetite refers to the amount of risk that the Bank is willing to take to achieve its strategic objectives; can be quantitative and/or qualitative in nature; naturally, risk appetite is lower than risk capacity.

- **Risk Limit:** Thresholds defined in relation to specific risk exposures that aim to contain the risk exposures undertaken by the organization below an acceptable level; limits can be established at the request of either the Board and/or management; limits should not be violated, and if breached result in mitigating actions to bring back to an acceptable level.

- **Risk Indicators / Risk Metrics:** Numerical targets defined in relation to specific risk exposures that aim to inform on risk positions across the Bank; they help measure, monitor and adjust, as necessary, the actual risk positions against expressed risk appetite and facilitate communication to key stakeholders.

- **Risk Owner:** Risk owners are the accountable point of contact for a risk at the senior leadership level, who oversee efforts to mitigate and manage the risk; risk owners typically are part of the first line of defense.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outline ABS's Policy with respect to the implementation, management, monitoring, and compliance with the Risk Management Framework ("RMF"). Risk Management looks across the organization and helps the Bank identify, evaluate and address the strategic, financial and operational risks that it faces, in order to minimize the negative effects on capital and earnings. The Risk Management Framework establishes oversight, control and discipline to drive continuous improvement of the Bank's risk management capabilities in a changing operating environment. The Risk Management Framework advances the maturity of the Bank's capabilities around managing its largest and most impactful risks.

2. Objectives

The Risk Management Framework formalizes a consistent Bank-wide approach to risk management. The document seeks to establish Bank-wide roles and responsibilities in the context of risk appetite, outlines the standards expected across the organization and formally defines key terms and concepts.

3. Key Components of Policy

Risk Management relies on multiple key reviews, metrics and Bank-wide taxonomies to perform its mission (see Figure 1 for key components in the Enterprise Risk Management Framework). Descriptions for the most important RMF components are described in the sections below.

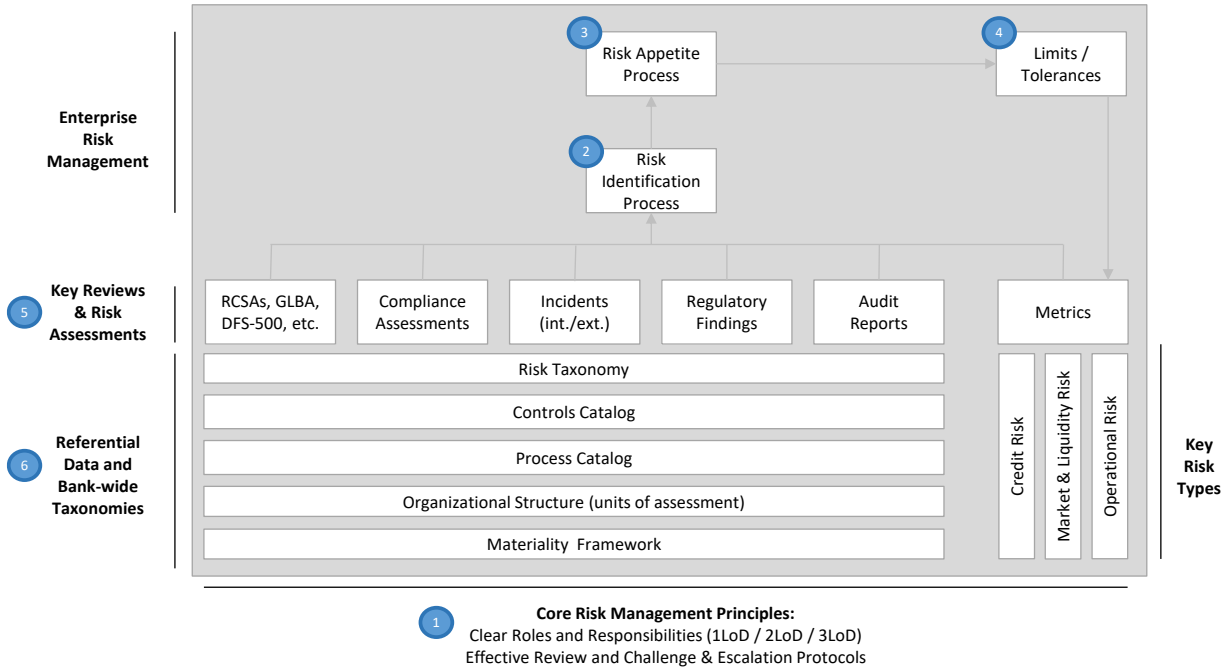

Figure 1: Enterprise Risk Management Framework

1) Core Risk Management Principles

1.1 Risk Culture - The Bank and senior management strive to set clear and consistent expectations for managing risks, including proactively self-identifying risk and control weaknesses (e.g., operational risk incidents, regulatory violations, security breaches, and data quality issues) and discussing tolerance of risks. Senior management actively seek out information about risks, promote adherence to limits, and encourage open and honest discussion about risks.

Senior management is clear about their accountability for managing business risks and the responsibilities of those that report to them for managing business risks. Management seek out risk information to support decision making, and the Bank's willingness to take on risk is understood and cascaded to staff.

Senior management encourage timely, efficient and effective communication of risk information across the organization, and risk events are seen as an opportunity to learn and take appropriate action to ensure the event does not reoccur.

1.2 Review and Challenge – The second line of defense (i.e., Risk Management Department, Compliance Department, Financial Crime Compliance ("FCC") is required to obtain a thorough understanding of the businesses it supports and the businesses' corresponding risk profile, to ask probing questions of management and to ensure senior management's actions prudently address risks.

Review and challenge is required for all of the risks facing the Bank, including but not limited to:

- Risk Limits and Exposures

- Internal Risk Incidents
- Risk and Control Self Assessments ("RCSAs")
- Control Assessments
- Models and Assumptions
- Vendor Outsourcing
- New Products and Major Change Initiatives

Review and challenge must be evidenced in risk meeting minutes (i.e., MRC and its sub-committees) and in risk reviews (i.e., RCSAs, Compliance Risk Reviews, incident reviews, new business approvals, etc.).

1.3 Risk Governance – Risk governance is designed to ensure clear accountability for monitoring risk and capital and escalating breaches of key limits (see Section III.3.4 for additional details on Risk Limits policy), thresholds and risk events as applicable.

The Board of Directors has delegated authority of risk management oversight to the Board Risk Committee ("BRC"). The BRC in turn relies on the Management Risk Committee ("MRC"), the most senior management committee in charge of managing the Bank's risks, to keep the BRC appropriately informed of risk issues (see Figure 2 below: Governance Hierarchy and Escalation Path for Risk Events). The MRC is charged with managing key issues and items related to administration of the Bank's risk management framework and functions, setting risk appetite, and establishing supporting processes.

1.4 Risk Events and Escalation – Timely identification and escalation of potential issues, incidents and/or breaches of established risk limits (a.k.a. "risk events") *upon detection* is the responsibility of *both* the first line of defense and second line of defense (see Section III.3.4 for additional details on Risk Limits policy).

Upon detection, risk events should be escalated to the Risk Management Department and the Chief Risk Officer ("CRO"), and should lead to prompt corrective actions to reduce risk to acceptable levels.

After corrective actions are taken, analysis into the root cause of the risk event should be undertaken. Analysis should explore the reason for and nature of the event (i.e., willful vs. negligent vs. unintentional), with an understanding that willful violation of policies and procedures may result in disciplinary action, up to and including termination. Risk events and associated analysis should be escalated to an appropriate risk management governance forum (i.e., MRC and/or its subcommittees) for review and potential further escalation (see: Figure 2).

Figure 2: Governance Hierarchy and Escalation Path for Risk Events

2) Risk Identification Process

Risk Identification is the Bank's systematic effort to identify and document the key risks, or top risks, the institution faces as a result of bank activities and its operating environment. The objective of Risk Identification is to understand what is at risk within the context of the Bank's explicit and implicit objectives and activities, and to generate a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or hinder the achievement of the Bank's strategic objectives.

The Risk Identification process is led by the Risk Management Department, conducted at least annually, developed with input from both the first line of defense and second line of defense, and refreshed on a periodic basis as necessary.

The Risk Identification process leverages: RCSAs, Compliance risk assessments, FCC data, audit reports, internal and external incident data, regulatory findings and risk metrics. The Risk Identification process leverages the Bank's Materiality Framework (see: Section III.3.6.1 - Materiality Framework) to ensure both risk impact and likelihood are examined in a consistent manner against established levels. The Risk Identification process also includes review of emerging risks and their materiality for the Bank.

The output of the Risk Identification process is a source of information to report the key risks throughout the Bank, as well as to key stakeholders. The output of the Risk Identification process is reported to both the MRC and BRC. Management uses the output of the Risk Identification process to focus their risk remediation priorities, and in the risk appetite process (see: Section III.3.3 – Risk Appetite).

3) Risk Appetite

Risk Appetite connects the Bank's strategy with its risk management Policy by defining the amount of

risk the bank is willing to take. The Risk Appetite Statement is a written statement of the main risk tolerances for achieving overall bank goals, and it explains the approach to managing these risks.

The objective of the Risk Appetite process is to understand and consider, in broad terms, the type of risks that the Bank would intend to take, to minimize or to avoid over short-, medium- and long-term time horizons. Risk Appetite helps inform how appropriate risk limits should be set in order to achieve an appropriate balance between risk and return in the context of the overall strategy of the Bank.

The Risk Appetite process leverages the results from the Risk Identification process. The output of the Risk Appetite process is a statement summarizing the Bank's accepted tolerances for risk taking activities across all risk types.

The Risk Appetite process is led by the Risk Management Department and conducted at least annually. The output of the Risk Appetite process results in the Bank's Risk Appetite Statement. The Risk Appetite Statement is approved annually by the BRC. After ratification, the Risk Appetite Statement is socialized within the organization, posted on the Bank's intranet site, used for limit setting process and monitored periodically throughout the year by the Risk Management Department.

4) Risk Limits, Risk Indicators and Metrics

4.1 Limits – Risk limits are thresholds defined in relation to specific risk exposures that aim to contain the risk exposures undertaken by the organization within an acceptable level. Limits can be established at the request of either the Board ("Board Limits") and/or Management ("Management Limits").

Limits should be established with consideration of the Bank's risk capacity and risk appetite to ensure that the Bank has sufficient capital and liquidity to operate normally during both periods of economic growth as well as periods of economic stress while at all times exceeding regulatory minimums. Additionally, limits should be set at levels that would not result in a violation of legal lending limits as promulgated by the New York State Department of Financial Services.

Board Limits are established by the Board. Board Limits should not be violated, and if breached, should result in mitigating actions to bring the risk back to an acceptable level. Board Limits should be calibrated to enable the Bank to withstand a severe economic stress and exceptional situations to continue to perform the Bank's primary business of taking in deposits and making loans to its customers. Board Limits are monitored by *both* the risk owners and the second line of defense, and reported at risk management meetings and the BRC. Violation of Board Limits is considered a more severe transgression than a violation of Management Limits.

Management Limits are proposed by the first line of defense risk owners or second line of defense, and approved by the second line of defense (Risk Management Department), consistent with the Bank's Risk Appetite Statement. Management limits must fall within the Board Limits set by the BRC to ensure that the Bank is operating within its stated Risk Appetite at all times. Management Limits should be calibrated to enable the Bank to withstand an expected level of economic stress during a normal business cycle. Management Limits are monitored by *both* the risk owners and the second line

of defense, and reported at risk management meetings.

Management Risk Limits can be adjusted (subject to Section III.3.4.1.2 below) at any time, but should be reviewed for potential change following the annual Risk Appetite setting process.

4.1.1 Monitoring Limits - Limits are monitored using the "traffic light" concept in the reporting process or, depending on the severity in the case of a breach (see below for definition of a "breach"), in notification to the respective governance bodies. Management should establish RAG levels for all risk limits. Amber levels should be established with enough time following initial detection of exposure movement out of risk appetite to allow for a course correction. For risk metrics and indicators where no specific limits have been set, any adverse development or trends will be highlighted.

- **Green**: Normal operating level; business as usual
- **Amber**: Warning level requiring heightened management review and potential escalation
- **Red**: Mandatory escalation and, for limits, reduction of risk

4.1.2 Risk Limit Breaches - For purposes of limit monitoring, a "breach" occurs when a limit enters into the Red zone. The purpose of establishing Green, Amber and Red levels allows Management and the Board to closely monitor and take mitigating action before an actual breach occurs. It is a goal of Management to not have any surprise breaches that are detected after the breach occurs.

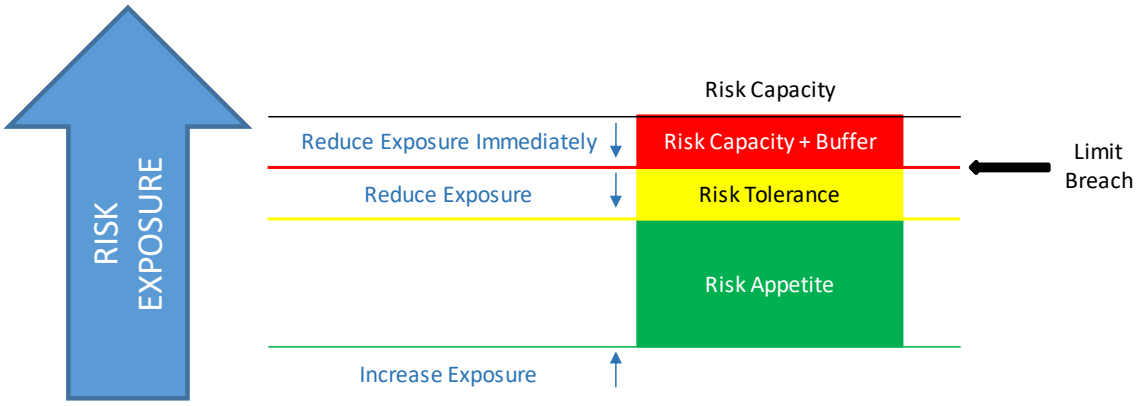

Figure 3: Key Limit Concepts and Corrective Actions

Due to the calibration approach taken when establishing limits, it is expected that breaches of Board Limits should seldom, if ever, be breached. On the other hand, breaches of Management Limits can be expected to occur from time to time.

Upon detection, risk limit breaches (entering into the "Red" zone) should be promptly escalated to the Risk Management Department and the CRO. Management Limit breaches must be reported to the MRC. Board Limit breaches must be reported to both the MRC and the BRC. All limit breaches should include root cause analysis explaining why the limit breach occurred, corrective actions taken to mitigate the risk, and monitored until actions are completed. It is further recognized that limit breaches can be willful or unintentional, and analysis of breaches should consider the nature of the

event. Disciplinary action will be considered for willful limit breaches. (See: Section III.3.1.4 Risk Events and Escalation).

4.1.3 Limit Adjustments - Risk owners may adjust a Management Limit; however, changes in limits must:

- be requested in advance of any breach (i.e., cannot be retro-active),
- obtain approval of the second line of defense (i.e., CRO),
- include a business and/or risk justification for the change,
- if temporary, have a predetermined date for return to the previously established limit, and
- cannot violate prudential regulations (i.e., legal lending limit, minimum capital ratios, etc.).

All adjustments in Management Limits must be reported to the MRC or the appropriate sub-committee.

4.2 Risk Indicators / Risk Metrics – Risk Indicators / Risk Metrics (a.k.a. Key Risk Indicators "KRI", Key Performance Indicators "KPI") are numerical targets defined in relation to specific risk exposures that aim to inform on risk positions.

Risk Indicators are established by either the first line of defense risk owners, or the second line of defense. Risk Indicators are monitored by either the risk owners or the second line of defense, and reported in risk management meetings.

5) Key Reviews and Risk Assessments

5.1. Risk & Control Self-Assessment - Risk & Control Self-Assessments ("RCSA") is a process by which management and staff of all levels jointly identify and evaluate risks and associated controls of key business lines and processes.

RCSAs are owned by the first line of defense and business process owners, and are reviewed and challenged by the second and third lines of defense. Operational Risk facilitates the RCSA process, ensuring alignment to the Risk Management Framework and related components.

The Bank's Business Process Owners perform and update RCSAs across key business units and processes at least annually, subject to management discretion and consultation with the business lines. This may result in an RCSA to be performed biannually due to key business priorities or an RCSA that has a residual risk of low. The detailed processes and requirements for conducting RCSAs are defined in the Bank's Operational Risk Policy and related procedure documents.

5.2 Internal Risk Incidents - Internal operational risk incidents are incidents that impact the Bank and occurred within the bank or a third-party / outsourcing entity the Bank has contracted services from.

Internal operational incident data provides meaningful information for assessing the Bank's exposure to operational risk and the effectiveness of controls. Incident data is used as input for RCSAs and the Risk ID process.

Incidents resulting in material loss and 'near misses' (i.e., incident was identified but secondary controls caught the error and was remediated resulting in no impact or financial loss) must be reported by the first-line of defense to Operational Risk in a timely manner and recorded by the first-line of defense in the Bank's GRC system. The detailed process and requirements for reporting internal incidents are defined in the Bank's Operational Risk Policy and related procedure documents.

5.3. Other Risk Assessments - Many functional areas (i.e., Compliance, FCC, Internal Audit, Technology, Chief Information Security Officer ("CISO"), etc.) perform reviews related to risks impacting the Bank (i.e. GLBA, DFS-500, etc.). These other risk assessments are considered in the activities outlined in this Risk Management Policy (i.e., Risk Identification, RCSA, Risk Appetite, etc.), but are governed through their own departmental policies and procedures. Where possible, alignment with the Materiality Framework and taxonomies outlined in Section III.3.6 of this document is encouraged.

5.4 Controls Testing – Controls testing is a procedure employed to ascertain the effectiveness of a control used to mitigate risk. Controls testing is performed by resources independent from those individuals or staff executing the control being tested. First-, second-, and third-lines of defense may perform controls testing as part of business-as-usual practices and as part of key reviews (e.g., Compliance Risk Assessments, RCSAs, FCC reviews and Internal Audits, etc.). The detailed processes and requirements for conducting control testing are defined in the individual department procedures. Information about controls and their effectiveness are stored in the Bank's GRC tool.

5.5 Issues Management – The first line of defense and business process owners are responsible for timely self-identification, disclosure and reporting of risk and compliance issues, including, but not limited to:

- Internal Risk Incidents
- Potential Loss Reports
- Regulatory Compliance Violations
- Security and System Breaches
- Privacy Breaches
- Data Issues
- Other Potential Control Issues

Issues should be recorded by the first-line of defense in ServiceNow, GRC and/or Continuity. The second line of defense should review issues identified to help identify root cause, understand organizational impacts and define remediation steps.

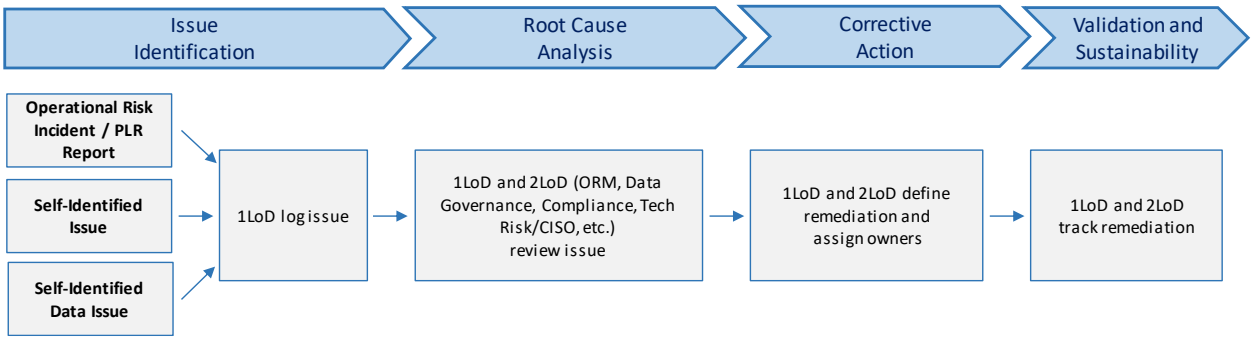

Figure 4: Issue Management Lifecycle

Through structured reviews (e.g., RCSA, credit risk reviews, model risk reviews, information security risk assessments, etc.) the second line of defense functions might identify issues. Issues and remediation actions identified by Risk Management teams should be loaded into the Bank's GRC tool. Material issues and actions, along with status, should be reviewed at appropriate Committee/Sub-Committee. Risk Management teams should review closing support documentation for material issues and actions prior to closing in the GRC tool.

6) Referential Data and Bank-wide Taxonomies

The Bank leverages several common libraries and taxonomies for processes, risks, controls and materiality, which are jointly owned and managed by the Risk Management, Compliance and Internal Audit Departments, and used in related assessments (e.g., RCSAs, audit reports, compliance reports, etc.) and metrics. These libraries reside in the Bank's GRC tool.

6.1. Materiality Framework - The Materiality Framework provides the Bank, including senior management and governing bodies, with a consistent mechanism for categorizing the materiality of risks. It is defined on an impact and likelihood assessment scale which defines materiality with regards to financial impact, non-financial impact, and likelihood estimate of occurrence (see: Figure 5 below).[♦♦] The Materiality Framework is leveraged in the RCSA, Risk Identification process, Risk Appetite process and other foundational reviews (see: Section III.3.2 - Risk Identification).

The bank defines material adverse impacts as Very High and High financial and nonfinancial categories.

6.2 Risk Taxonomy – The Risk Taxonomy is a common way of organizing and aggregating risk information across Risk, Compliance and Internal Audit reviews (see: Figure 6 below). The Risk Taxonomy is leveraged in the RCSA, Risk Identification process, Risk Appetite process and other foundational reviews. The common taxonomy helps the Bank categorize, organize and aggregate information across the organization.

♦♦ The thresholds defined in the Materiality Framework are expected to both evolve and become more granular with wider adoption and usage over time and will be updated in this document accordingly

Materiality Framework During Normal Situations

	Frequency		Financial Impact		
	Possible / Adverse Stress	Probable / Baseline Conditions	Profit and Loss Impact	Core Equity Impact (CET-1)	Balance Sheet Impact
Frequency Definition:	Event may occur over a business cycle (e.g. within 5~10 years)	Event occurs in business-as-usual situations (e.g. every year)			
Impact	VH	VH	>$5mm (~ 5% Earnings)	> 50 bps	> 5%
	H	H	$2mm - $5mm	20 bps - 50 bps	2% - 5%
	M	M	$1mm - $2mm	10 bps - 20 bps	1% - 2%
	L	L	< $1mm	< 10 bps	< 1%

	Frequency		Non-Financial Impact		
	Possible / Adverse Stress	Probable / Baseline Conditions	Regulatory Impact	Customer Impact	Reputational Impact
Impact	VH	VH	Significant regulatory scrutiny; potential loss of business license; significant fines	Significant impact / loss of customers; likely litigation / compensation claims; significant loss of deposits	Trustee impact, deterioriation of Bank owner's value
	H	H	Regulatory scrutiny; possible legal action/regulatory fines; likely to result in improvement order	Potential financial detriment to customers / loss of customers	Negative media coverage in general public
	M	M	Internal compliance issues; possibly reportable to regulator; could result in improvement order	Moderate impact to customers, limited to a relatively small number	Negative coverage within industry
	L	L	Disciplinary warning; minimal regulator action	Minimal potential for customers impact	Negative press unlikely

Materiality Framework During Exceptional Situations

	Frequency	Financial Impact		
	Remote / Severe Stress	Profit and Loss Impact	Core Equity Impact (CET-1)	Balance Sheet Impact
Frequency Definition:	Event occurs in exceptional situations (e.g. tail risk, beyond 10 years)			
Impact	VH	>$10mm (~ 10% Earnings)	> 100 bps	> 10%
	H	$4mm - $10mm	40 bps - 100 bps	4% - 10%
	M	$2mm - $4mm	20 bps - 40 bps	2% - 4%
	L	< $2mm	< 20 bps	< 2%

Figure 5: Materiality Framework

L1	LEVEL 1	L2	LEVEL 2
1.0	Credit Risk		
		1.1	Counterparty
		1.2	Concentration
		1.3	Settlement
		1.4	Collateral / Credit Mitigation
2.0	Liquidity Risk		
		2.1	Funding Liquidity
		2.2	Non Traded Market
3.0	Capital Risk		
		3.1	Capital Adequacy
4.0	Market Risk		
		4.1	Interest Rate
		4.2	Foreign Exchange/Currency
		4.3	Equity
		4.4	Commodity
5.0	Model Risk		
		5.1	Intrinsic Uncertainty
		5.2	Model Design
		5.3	Model Usage
		5.4	Model Documentation
		5.5	Model Validation
6.0	Business Risk		
		6.1	Failure to Meet Earnings Target
		6.2	Failure to Adapt to Long-Term Strategic Trends
		6.3	New Business and Change Management
		6.4	Investment
7.0	Reputational Risk		
		7.1	Product
		7.2	Environmental
		7.3	Societal
		7.4	Governance
8.0	Operational Risk		
		8.1	Financial Crime
		8.2	Compliance
		8.3	People and Conduct
		8.4	Processes
		8.5	Systems
		8.6	Third-Party (Suppliers, Vendors and Outsourcing)
		8.7	Cyber
		8.8	Resiliency

Figure 6: Risk Taxonomy ♦

4. Escalation Procedures

The Policy Owner will monitor this Policy. Any non-compliance with this Policy will be escalated to the Designated Management Committee for resolution. If the Designated Management Committee cannot resolve the issue, it will be escalated to the Executive Management Steering Committee

♦ Note: Figure 6 above is illustrative as Level-3 risks in the taxonomy are not shown

("EMSC") for further consideration. If the issue cannot be resolved by the EMSC the issue will be escalated to the Board or Designated Board Committee for further consideration.

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE

Required Annual (12 Month) Board Review and Approval Cycle (Policy Level 1)

The Policy Owner is responsible for initiating the Board review of this Policy on an Annual basis prior to the Next Board Review Date. The Policy Owner will track the Next Board Review Date for this Policy and begin the review process early enough to provide ample time for all necessary approvals to occur in a timely manner.

Once the updated Policy has been approved by the Designated Board Committee (or the Board, as the case may be), the updated Policy shall go into effect and the Policy Owner shall be responsible for delivering the approved Policy document to the PPA within seven days of the approval date so that it can be loaded in a timely manner to AppleNet or such other intranet site where Policies are stored and made available to the employees of the Bank. The Next Board Review Date shall be adjusted accordingly.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

Off-Cycle Policy Changes – Review and Approval Process (Policy Level 1)

If the Policy requires changes to be made outside the required Annual Regular Board Review Cycle noted in the previous section, the Policy shall be updated by the Policy Owner, in consultation with the Legal Contact.

If the changes are Immaterial Changes (i.e., no change to any substance of the policy, but rather grammar, formatting, template, typos, etc.), such changes shall be submitted to the Designated Management Committee for approval and no further approval is required. A record of all such changes shall be kept and submitted for reference to the Designated Board Committee (or the Board, as the case may be) during the required Annual approval cycle (or the next time the Policy requires interim Board approval, whichever comes first).

If the changes are Material Changes (i.e., changes that would materially alter the substance of the Policy in any way), the revised Policy shall be submitted to the Designated Management Committee for approval and recommendation to the Designated Board Committee (or the Board, as the case may be) for final approval. Final approval by the Designated Board Committee in this instance shall be required. To the extent the Designated Management Committee is a sub-committee, prior to review by the Board or Designated Board Committee the updated Policy shall be reviewed by the primary management committee with oversight of the Designated Management Committee. If the Designated Management Committee cannot agree on an issue or a change to the Policy, it shall be submitted to the EMSC for consideration.

Once the steps above are complete and the Policy has received final approval by either the Designated Management Committee or the Designated Board Committee (or Board, as the case may be), the updated Policy shall go into effect and the Policy Owner shall be responsible for

delivering the approved Policy document to the PPA within seven days of the approval date so that it can be loaded in a timely manner to AppleNet or such other intranet site where Policies are stored and made available to the employees of the Bank.

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW

Risk Management, in consultation with Legal, identifies the Designated Management Committee, Designated Board Committee (or the Board, as appropriate), and Policy Level for this Policy, and re-evaluates the same at least Annually. Changes, if any, will be communicated to the Policy Owner, who shall update the Policy accordingly, as well as the PPA.

VII. EXCEPTIONS TO THE POLICY

Requests for exceptions to this Policy must be specific and may only be granted on specific items, rather than to entire sections. Any exception to this Policy must be made in accordance with the requirements set forth in Apple Bank's Exception Policy.

VIII. RETIREMENT OF POLICIES

In the event this Policy needs to be retired or merged with or into another Policy, the Policy Owner must notify the PPA and provide a rationale for the proposed retirement or merger. The Bank's General Counsel and Chief Risk Officer will review the rationale and determine whether the requested action is appropriate. Notice of retired Policies shall be provided to the Board or relevant Designated Board Committee on a semi-annual basis.

IX. ROLES AND RESPONSIBILITIES

Chief Executive Officer ("CEO"): The CEO drives the risk culture and supports the Risk Management Framework by ensuring that risk appetite is embedded within the Bank's decision making processes. The CEO collaborates with the CRO to ensure management is held accountable for the integrity of the Risk Management Framework, including three core areas: 1) framework development, 2) risk planning and calibration, and 3) monitoring compliance. The CEO ensures suitable capabilities are available to implement the Risk Management Framework.

First Line of Defense / Business Process Owners ("1LoD"): The first line of defense is responsible for risk identification and management on a front-to-back basis, including design, operation and testing of controls required to comply with risk appetite and policies, self-identification of control issues, data issues and incident reporting. The first line owns the risks generated by the business activities.

Chief Risk Officer ("CRO"): The CRO collaborates with CEO to drive the risk culture and ensure management is held accountable for the integrity of the Risk Management Framework, including three core areas: 1) framework development, 2) risk planning and calibration, and 3) monitoring compliance. The CRO chairs the Management Risk Committee, recommends strategic risk objectives to the Board and drives the Board Risk Committee agenda.

Management Risk Committee ("MRC"): The MRC is the most senior management committee overseeing the Bank's risks. The Committee receives its authority from the Board Risk Committee and is charged with managing key issues and items related to administration of the Bank's risk management Policy and functions, setting risk appetite, and establishing supporting processes.

Second Line of Defense / Risk Management Department / Chief Information Security Office ("2LoD"): The second line of defense is responsible for establishing risk management standards and providing independent review and challenge of activities, processes and constraints carried out by the first line, incidents reported and risks identified by the first line of defense (see section 1.3 Review & Challenge).

Compliance Department / Financial Crimes Compliance ("FCC"): The Compliance Department and FCC are second line of defense functions, and are responsible for ensuring that the Bank complies with applicable laws, regulations and rules. Compliance, FCC and CISO play an essential role in helping to preserve the integrity and reputation of the Bank.

Third Line of Defense / Internal Audit ("3LoD"): Internal Audit is the Bank's third line of defense, and plays a role in evaluating the effectiveness of internal constraints related to all Bank activities. Assessments are performed covering front-to-back business flows with consideration of all relevant risks in accordance with their respective policies.

Bank Personnel: Bank Personnel are responsible for understanding and following relevant Policies. Bank Personnel participate in the development or updates of Policies that exist within their business unit. When creating or updating Policies, Bank Personnel should follow the PPGP and utilize the associated Policy template which is available on AppleNet.

Executive Management Steering Committee (EMSC): To the extent necessary, the EMSC shall consider matters that cannot be decided by the Designated Management Committee.

Senior Management: Members of management and business units are responsible for implementing this Policy, ensuring compliance and understanding of this Policy as well as developing procedures for his/her unit, to the extent needed, that align with the requirements of this Policy.

Internal Audit: The Internal Audit team is responsible for the periodic audit of this Policy. Internal Audit will review the processes and any related gaps will be identified as findings to be monitored and remediated.

Legal Contact: See Section II – Definitions.

Policies and Procedures Administrator ("PPA"): See Section II – Definitions.

Policy Owner: See Section II – Definitions.

Risk Management: Risk Management, in conjunction with Legal, determines the initial Designated

Management Committee, Designated Board Committee (or Board, as appropriate), and Policy Level of the Policy and the Regular Board Review Cycle for this Policy, and re-evaluates the same at least Annually.

X. RECORD RETENTION

Any records created as a result of this Policy should be held pursuant to the Bank's Record Retention and Disposal Policy. Should records created as a result of this Policy require a different retention period (either a shorter or longer time period), the Policy Owner (in conjunction with the relevant business area leader) must describe the rationale for a different retention period and share the rationale with the Designated Management Committee.

XI. QUESTIONS AND CONTACT INFORMATION

Questions regarding compliance with this Policy may be addressed to the Policy Owner listed in the tracking chart on the first page.

XII. LIST OF REFERENCE DOCUMENTS

None

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
4.2	12/14/2020	Replaces: Apple Financial Holdings, Inc. and Apple Bank for Savings - Risk Management Framework as of December 2019 Change includes edits to section 6.1 where the Bank defines material adverse impacts Defines GRC tool	Richard Leite	MRC and BRC
4.3	11/17/2021	Added Addendums # 1 and #2 to the main body of the Risk Management Framework Updated to current policy template	Richard Leite	MRC and BRC