Apple Financial Holdings, Inc.

Operational Risk Management Policy

November 17, 2021

Contents

I. POLICY PURPOSE STATEMENT AND SCOPE 4

II. DEFINITIONS 4

III. KEY POLICY COMPONENTS 5
1. Executive Summary 5
2. Objectives 5
3. Key Components of Policy - Operational Risk Management Framework Components 6
3.1 Internal Incident Data Collection 6
3.2 Risk and Control Self-Assessment (“RCSA”) 7
3.3 Controls Testing 7
3.4 Issues and Actions Management 7
3.5 Key Risk Indicators (“KRI”) / Key Performance Indicators (“KPI”) 8
4. Escalation Procedures 8

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE 8

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS 9

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW 9

VII. EXCEPTIONS TO THE POLICY 9

VIII. RETIREMENT OF POLICIES 9

IX. ROLES AND RESPONSIBILITIES 9

X. RECORD RETENTION 11

XI. QUESTIONS AND CONTACT INFORMATION 11

XII. LIST OF REFERENCE DOCUMENTS 11

XIII. REVISION HISTORY 12

REVIEW AND TRACKING CHART

Effective Date*:	November 17, 2021
Version Number:	3.0
Policy Level:	Policy Level 2
Corresponding Board Review Frequency:	Biennial (Every 24 Months)
Board or Designated Board Committee:	Board Risk Committee (“BRC”)
Last Board Review Date*:	November 17, 2021
Next Board Review Date*:	November 2023
Designated Management Committee:	Management Risk Committee (“MRC”)
Last Management Review Date*:	November 4, 2021
Next Management Review Date*:	November 2022
Policy Owner:	Betty Sellinger, FVP, Operational Risk Management

I. POLICY PURPOSE STATEMENT AND SCOPE

The Operational Risk Management Policy (the "Policy") applies to the management, monitoring and governance of operational risk 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.

- **Biennial or Biennially:** Every twenty-four (24) months.

- **Coversheet:** The form to be submitted to the PPA (defined in this Section) in connection with revised Policies, Standards, Procedures, or Manuals. The Coversheet 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.

- **Key Risk Indicators ("KRI") / Key Performance Indicators ("KPI"):** 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.

- **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; 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.

- **Operational Risk**: The risk of loss resulting from inadequate or failed processes, people, and systems or from external events.

- **Policy Level 2:** A Regular Board Review Cycle level for a Policy, designated by Risk Management in consult with Legal. Level 2 policies require Biennial approval by the Board or a Designated Board Committee.

- **Policy Owner:** The person responsible for management and tracking of the Policy. This includes initiating the review of the 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 Policies and Procedures Administrator ("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.

- **PPA (Policies and Procedures Administrator):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Policy and Procedure reviews, obtains the updated versions of Policies and Procedures, and ensures 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 Board level committee approval process for a Policy, the frequency of which is determined by the designation of Level 1, Level 2, or Level 3.

- **Risk Management Framework:** 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.

III. KEY POLICY COMPONENTS

1. Executive Summary

This document outlines ABS’s Policy with respect to the management, monitoring, and governance of operational risk. To mitigate such risks, Operational Risk Management (“ORM”) has established a program that centralizes, formalizes and leverages industry best practices. It provides the Bank with the necessary tools to identify, assess, manage, monitor, and report the risks encountered through the Bank’s daily business, while meeting regulatory expectations.

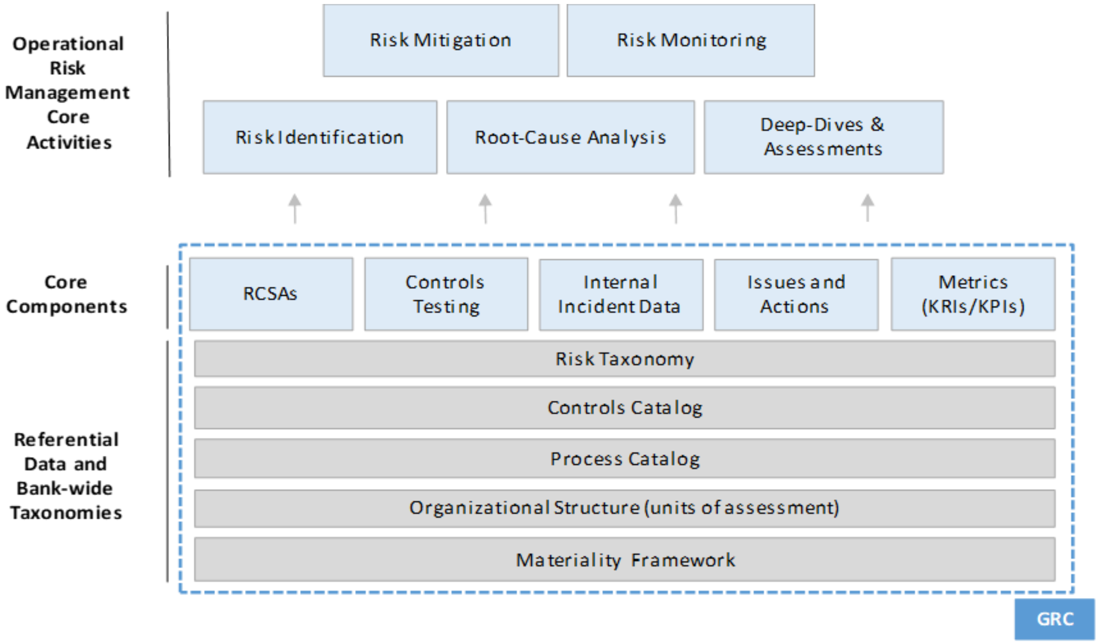
2. Objectives

The objective of the Policy is to define the framework for identifying, assessing, mitigating, monitoring, and reporting on operational risk throughout the Bank, in a manner consistent with the Risk Management Framework. This Policy provides a comprehensive governance structure for managing operational risk and for the identification and evaluation of threats that may arise during the normal course of business or in response to market events. The Policy includes protocols for reporting, escalation, and remediation of operational risk incidents and potential exposures.

As described in the Risk Management Framework, review & challenge is required within the second line of defense to obtain a thorough understanding of the businesses it supports and the businesses' corresponding risk profile and to ensure senior management's actions prudently address risks.

See Figure 1 for key components in the Operational Risk Management Framework.

Figure 1: Operational Risk Management Framework



Detailed descriptions of the key Operational Risk Management Framework components are described below.

3. Key Components of Policy - Operational Risk Management Framework Components

3.1 Internal Incident Data Collection

As described in the Risk Management Framework, internal operational risk incidents are those operational risk incidents that impact the Bank and occur within the Bank or a third-party / outsourcing entity with whom the Bank has contracted services[11]. Internal operational incident data provides meaningful information for assessing the level of risk, showing where the Bank may have exposure and where controls may be ineffective.

The incident collection process establishes consistent minimum requirements for all the business units to follow for collecting, classifying, reporting and reviewing incidents resulting from operational risk events. Incident data is used as input for RCSAs, Risk Identification, and Issues and Actions processes.

All business-line employees are responsible for pro-actively self-identifying and escalating risk and control weaknesses (e.g., operational risk incidents, near misses, etc.) on an ongoing basis. Incidents resulting in material loss and "near misses" (i.e., an

[1] This includes sub-servicers (fourth party vendors) contracted by the Bank's vendors.

incident was identified but secondary controls caught the error and was remediated resulting in no impact or financial loss) must be reported by the business unit to ORM in a timely manner and recorded by the business unit in the Governance, Risk and Compliance ("GRC") tool, the Bank's system of record for risk issues and incidents. Business unit management is responsible for ensuring that all incidents within their department are submitted in accordance with this Policy. The business is required to work with ORM on the root cause analysis and develop appropriate action plans to mitigate against exposure to future potential risk incidents by enhancing their control environment. ORM reviews, validates, and escalates the incidents as necessary. ORM generates trending and other risk analysis across all businesses to produce centralized reports, enhancing the ability of management to make decisions regarding risk mitigation.

3.2 Risk and Control Self-Assessment ("RCSA")

As described in the Risk Management Framework, the RCSA is a process by which management and staff of all levels collectively identify and evaluate risks and associated controls of key business lines and processes. The Bank's business lines perform and update RCSAs across key business units and processes at least annually, subject to management discretion. This may result in an RCSA being performed biannually due to key business priorities or an RCSA that has a residual risk rating of low. RCSAs are owned by the first line of defense and business process owners, and are reviewed by the second and third lines of defense.

ORM facilitates the RCSA process, which is an integral part of the Bank's overall Operational Risk Framework. The RCSA serves as the Bank's inventory of key operational risks and controls as defined by the business units and their respective risk levels. It also provides a means of identifying the operational risks and related control weaknesses that could result in high-risk exposures if not properly managed. Additional details related to the RCSA process are defined in the RCSA procedures.

3.3 Controls Testing

All three lines of defense may perform controls testing as a part of business-as-usual practices and as part of key reviews or ongoing monitoring. Control testing should be performed by resources independent from those individuals or staff executing the control being tested. The Controls Testing framework supports the overall RCSA, since control assessment ratings can be based on results of the assurance activity. It allows the Bank to identify, assess and monitor the effectiveness of the control environment. It provides management with assurance that the Bank's risks are being mitigated through the execution of appropriate and working controls. Additional details are defined in the Control Testing procedures.

3.4 Issues and Actions Management

Issues are defined as an action requiring mitigation or remediation, arising from either a material risk or an identified control deficiency. Within the ORM framework, issues may arise from action plans resulting from: an RCSA, root cause analysis of an internal incident, monitoring or breach of a KRI limit, or action plans resulting from the risk identification process that may impact the Bank's strategic objectives. ORM reviews issues identified to help determine root cause, impact and remediation steps. Issues and remediation actions identified by first line in conjunction with ORM should be loaded into the Bank's GRC tool.

Material issues and actions, along with status, should be reviewed at the MRC. If the action plan is not completed by the due date, the issue will be reported to the MRC. ORM should review closing support documentation for material issues and actions prior to closing in the GRC tool.

Issues should be self-identified by the first line of defense to support tracking of a known control issue.. All self-identified issues and action plans should be recorded by the first line of defense in GRC. Each action plan has appropriate detail to address the issue, and an assignment of an accountable owner and due date. The named accountable owner is responsible for the timely completion of their action plan(s), with adequacy of completion subject to review and approval by ORM and/or the control function raising the issue.

3.5 Key Risk Indicators (“KRI”) / Key Performance Indicators (“KPI”)

Key Risk Indicators (“KRI”) and Key Performance Indicators (“KPI”) are numerical metrics used to identify early signals of risk exposures. These metrics will identify and measure operational risks in a systematic way using objective data at the Bank and business unit level, based primarily on the risks identified under the operational risk framework process. Appropriate training will be provided to those Bank employees involved in this process prior to implementation of these reporting processes.

The first line of defense defines the measures of the risks within their business, and are responsible for identifying and owning relevant metrics, collecting associated data, and aligning this data with the risks and controls of their business. ORM facilitates a discussion with the business leveraging their subject matter expertise. When metrics exceed established targets or thresholds, ORM will work with the business to understand the root cause and determine a corrective action plan that will be recorded by the first line of defense in GRC as needed. These metrics and the appropriateness of targets or limits are evaluated by the business and ORM. Updates can be made at any time, but may be triggered by changes in the Bank or business operations.

4. Escalation Procedures

The Policy Owner will monitor this Policy. Any non-compliance with the Policy will be escalated to the MRC for resolution. If the MRC cannot resolve the issue, it will be escalated to the Executive Management Steering Committee (“EMSC”) for further consideration. If the issue cannot be resolved by the EMSC, the issue will be escalated to Board or BRC for further consideration.

IV. REQUIRED PERIODIC REVIEW AND APPROVAL CYCLE

(A) Required Biennial (24 Month) Board Review And Approval Cycle (Policy Level 2)

The Policy Owner is responsible for initiating a regular Board review of this Policy on a Biennial (every 24 months) 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.

(B) Required Annual (12 Month) Management Review (Policy Level 2)

This Policy shall be reviewed Annually by the Policy Owner, in consultation with the Legal Contact, and updated (if necessary).

Once the updated Policy has received final approval by either the Designated Management Committee or 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.

V. OFF-CYCLE REVIEW AND APPROVAL PROCESS

Off-Cycle Policy Changes – Review And Approval Process (Policy Level 2)

If the Policy requires changes to be made outside the Required Board Review Cycle outlined in the previous section, review and approval shall follow the Required Annual (12 Month) Management Review process outlined in Section IV(B) above.

VI. DESIGNATED COMMITTEES AND POLICY LEVEL REVIEW

Risk Management, in conjunction 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 comply with applicable laws/regulations and 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

The roles and responsibilities for ORM are in adherence to the “Three Lines of Defense” model, emphasizing that the identification, assessment, mitigation, monitoring and reporting of operational risk is the responsibility of all Bank employees, and that the principal objective of the operational risk framework is to assist the business with this responsibility as part of day-to-day operations.

Detailed descriptions of the key Operational Risk Management Framework roles and responsibilities are described below. Parts of the First Line of Defense and Second Line of Defense roles are referenced from the Risk Management Framework.

Business Units /Business Process Owners / First Line of Defense ("1LoD"): All business units and support functions within the Bank are responsible for the identification, assessment, mitigation and monitoring of operational risk exposures within their areas of responsibility. The management of operational risk is an ongoing responsibility and is part of the day-to-day operating roles of all employees.

Operational Risk Management Department / Second Line of Defense ("2LoD"): Operational Risk Management (ORM) is an independent risk management function and is primarily responsible for:

- Establishment, implementation and governance of the operational risk framework
- Ongoing monitoring of adherence to the ORM framework by the business units
- Analysis and reporting to senior management and the Board on bank-wide operational risk exposures, including timely escalation of risk exposures identified under the framework
- Support, advise, and provide training to the business with respect to the ongoing rollout and application of the framework

Head of Operational Risk Management: The Head of ORM reports to the Chief Risk Officer ("CRO"). To support the effective implementation of the operational risk framework, ORM's staffing consists of team members who are aligned with, but functionally independent of, the business units and support their implementation of the ORM framework components. ORM team members have independence from the business units they support and report to the Head of ORM.

Compliance Department / Financial Crimes Compliance ("FCC") / Chief Information Security Office ("CISO"): The Compliance Department, FCC and CISO are second line of defense functions, and are responsible for ensuring that the Bank complies with applicable laws, regulations and rules. Compliance and FCC play an essential role in helping to preserve the integrity and reputation of the Bank. Such functions are accountable for the implementation of frameworks intended to identify, manage, and remediate specific risk types within the overall definition of operational risk but which, due to their complex, specialized or specific nature, require dedicated support and focus to effectively manage. Where practical, such functions should provide reporting to ORM to support the aggregation and analysis of these specific risks within the context of the overall ORM framework.

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.

Designated Board Committee: The Designated Board Committee provides general oversight over management's administration of the Policy. The Designated Board Committee is responsible for initially approving this Policy and reviewing the Policy on a Biennial basis according to the Policy Level (refer to the Review and Tracking Chart).]

Designated Management Committee: The Designated Management Committee is responsible for reviewing and approving changes to the Policy as set forth herein on an Annual basis (except in the year designated for Board approval) and submitting Material Changes to the Designated Board Committee, or Board, as appropriate.

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.

Policy Owner: See Section II – Definitions.

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

Legal Contact: 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 re-evaluates the same at least Annually.

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.

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

- Operational Risk Management RCSA Procedures
- Operational Risk Management Controls Testing Procedures
- Governance, Risk and Compliance ('GRC") User Tool Manual

- Risk Management Framework Policy

XIII. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
2.0	12/3/2020	Revised for changes to the template, added more information under the Issues and Actions Management section, minor wording changes including the GRC tool.	B. Sellinger, FVP, Head of Operational Risk	MRC
3.0	11/17/2021	Revised to include edits to Section III.3.2 (RCSAs), additional GRC information, and changes to the template.	B. Sellinger, FVP, Head of Operational Risk	MRC, BRC