Apple Financial Holdings, Inc. / Apple Bank for Savings
Enterprise Business Continuity Policy

May 26, 2021

Contents

POLICY NAME: AFH Enterprise Business Continuity Policy

REVIEW AND TRACKING CHART

Effective Date:	May 26, 2021
Version Number:	4.0
Policy Level:	1
Corresponding Board Review Frequency:	Annual (Every 12 Months)
Board or Designated Board Committee:	Board Operations and Technology Committee
Last Board Review Date:	May 26, 2021
Next Board Review Date:	May 2022
Designated Management Committee:	Technology and Operations Planning Committee (TOPC)
Last Management Review Date:	May 25, 2021
Next Management Review Date:	May 2022
Policy Owner:	Debi Gupta, CTO David James, BCM / DR Leader

Terms not defined herein are defined on the Review and Tracking Chart on previous page.

I. POLICY PURPOSE STATEMENT AND SCOPE

The Business Continuity Policy (the "Policy") applies to the implementation, management, monitoring, compliance with Business Continuity Program at Apple Financial Holdings, Inc. ("AFH"), inclusive of Apple Bank for Savings and its subsidiaries (collectively, "ABS," "Apple," or the "Bank") in accordance with applicable state and federal statutes, rules and regulations.

All ABS employees must comply with the terms of this Policy to the degree applicable to them.

II. DEFINITIONS

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

- **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; 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 consult with Legal. Level 1 policies require Annual approval by the Board or a Board level 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") (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.

- **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.

- **Business Continuity Management (BCM) Program:** Ongoing management and governance process supported by top management and appropriately resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products and services through training, exercising, maintenance and review.

- **Business Continuity Plan (BCP):** A comprehensive plan that provides direction for the resumption of business process(s) in the event of a disruption.

- **Business Continuity Risk:** The risk of the disruption of business processes that are critical to the financial health, operation, regulation and/or reputation of Apple Bank.

- **Business Process Owner:** A person who is responsible for the process(s) contained in the document (BIA, BCP) and has the authority to allocate resources (time, people, finances), if required in order to support recovery of the business.

- **Business Segment:** Refers to the major operating units and, for the requirements outlined in Apple Bank's BCM Policy.

- **Business Continuity Management Leader:** The senior-most individual tasked with leading the development and execution of Apple Bank's Business Continuity Management Program.

- **Critical Process:** A process identified through the Business Impact Assessments or Business Impact Assessments as being significant in financial, operational, customer, regulatory, and/or reputational terms should it be disrupted.

- **Crisis Management:** The process of preparing for, and responding to, an event threatening life, health, property or security. One element of crisis management response is determining whether to invoke the applicable BC Plan.

- **Enterprise:** A term used to describe Apple Bank for Savings and its subsidiaries collectively.

- **Test or Exercise:** A planned event, whereby elements of a business continuity plan are tested to rehearse steps, confirm responsibilities, and otherwise ensure that business continuity plans, disaster recovery plans, and/or BCM Program capabilities are effective.

- **Apple Bank's BCM Program Office:** The function at Apple Bank responsible for leading the business continuity program and is led by the Apple Bank BCM Leader.

- **Independent Function:** A function comprised of individuals who are not stakeholders in the BCM Exercise Strategy and as such may be business continuity professionals from Internal Audit, or qualified third party. Other Independent Functions may include members of Operational Risk, Compliance and/or IT.

- **Inherent Risks:** Those internal or external risks to which the institution is exposed as a result of the business activities in which it engages and the external environment in which the activities take place. Inherent risk results from the processes, activities or transactions in which the institution is involved. Inherent risk includes risks that emerge with respect to existing businesses and activities, as well risks that emerge as the company enters new businesses or activities. Inherent Risk assessments do not, however, consider the mitigating effects of controls designed to address the risk being assessed.

- **IT Disaster Recovery:** The business process's technical systems (i.e., hardware, software, networks and related services) identified as required in the event of an outage. BCM should prioritize critical systems, applications and functions for recovery and agree upon targeted recovery times and acceptable data loss based on the BIA and associated costs to achieve the targets.

- **Loss Scenario:** The net result of an event to which plans are written to address.

- **Maximum Allowable Downtime (MAD):** The length of time within which a business process must be recovered to avoid significant impairment financially, operationally, or for legal/regulatory obligations. MAD time starts when a process becomes unavailable and stops when recovery is achieved.

- **Procedures:** A set of instructions developed to support a policy; the instructions detail the actions and tasks necessary to meet the requirements outlined in such policy.

- **Process:** A set of related tasks or activities that culminate in a product or service for a customer.

- **Quality Assurance:** Any systematic process of checking to see whether a product or service being developed is meeting specified requirements. A quality assurance system is said to increase confidence and credibility, improve work processes and efficiency, and enable a function to better compete with others.

- **Recovery:** Restoration of a disrupted process or resource (in contrast to business as usual).

- **Recovery Point Objective (RPO):** Point to which information used by an activity must be restored to enable the activity to operate on resumption.

- **Recovery Time Objective (RTO):** Time goal for the restoration and recovery of functions or resources based on the acceptance down time and acceptable level of performance in case of a disruption of operations.

- **Regulated Entities:** In the context of Apple Bank's BCM Policy, any subsidiary owned directly or indirectly, and is separately regulated at the entity level.

- **Residual Risk:** The level of risk remaining after applying the mitigating effect of risk controls to the applicable Inherent Risks. Implemented controls may include best practice control frameworks and regulatory compliance requirements.

- **Resumption:** The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified timeframes.

- **Resource:** A supply or source required by a disrupted process for recovery. Examples include: applications, systems, third party services and hardware.

- **Risk Based Testing:** Testing based on identification of potential risks which should be analyzed by the project stakeholder or which might appear during the project's development.

- **Segment:** A unit, subsidiary, P&L, division, platform, portfolio, or business unit.

- **Exercise/Test:** A planned event whereby elements of a business continuity plan are tested to rehearse steps, confirm responsibilities, and otherwise ensure that business continuity plans and/or BCM Program capabilities are effective.

- **Third Party:** Vendor, supplier, partner, contractor, service provider or customer.

- **Vital Vendor**: Bank non-affiliate and affiliate third-party vendors that have been evaluated against multiple risks and factors to determine the appropriate level of monitoring and oversight.

III. KEY POLICY COMPONENTS

1. Executive Summary

Business Continuity Management is a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

ABS manages its Business Continuity Program by establishing and implementing a policy and associated plans that help to ensure the availability of critical business processes. The Business Continuity Management (BCM) Plans must address the following risk management objectives for the Program:

- Development of an enterprise-wide program and the prioritization of business objectives and critical operations that are essential for business continuity.
- Alignment and coordination of both BCM & IT/DR responsibilities.
- Development and maintenance of BC Plans to provide for the recovery and resumption of potentially affected critical processes.

- Regular *(no less frequently than annually)* and as-necessary prepare updates to each BC Plan based on changes in Apple Bank's organizational structure or business processes covered by any such plan, audit or independent function recommendations, or lessons learned from validation exercises or actual events.
- Annual process-oriented approach that includes Business Impact Assessment ("BIA"), Risk Assessment ("RA"), recovery strategies and components documented in BC Plans, maintaining plans, training, and validation exercising.
- Leaders and employees trained and made aware of their roles in business continuity.

2. Objectives

This Policy defines the minimum requirements of the Business Continuity Program. Each Business Continuity Plan *(BCP)* will define:

- Business Impact Assessment *("BIA")* in the very least containing a process inventory, key dependencies & risk attributes.
- Recovery Strategies.
- RA.
- Test Exercises.
- Communication & Incident Protocol.
- Maintenance of this program.

Each BCP shall address how that line of business ("LOB") functions:

- Manages identified & controls various forms of business risks.
- Identifies & prioritizes essential personnel, & sufficient financial resources to properly implement the BCP.
- Ensures that BCPs are regularly validated through an exercise schedule.
- Identifies and tracks issues to closure.
- Ensures the Program is updated to reflect the current operating environment and meets both LOB functions and HQ regulatory requirements.

The enterprise-wide ABS BCM Program establishes the framework and tools to assist the Business in identifying their resiliency risk landscape and implementing mitigating strategies for this risk.

3. Key Components of Policy

Business Impact Assessments (BIA)

A BIA is essential to a BCM Program and must include both an assessment component to determine impacts, as well as the requirements to enable the development of strategies and plans for minimizing risk. One of the basic assumptions behind a BIA is that certain processes within a business are more crucial than others.

ABS employs a BIA process within each Business Segment as appropriate to:

- Identify, assess and prioritize business processes, including their interdependencies.
- Define the potential impact of business disruptions resulting from hazards and uncontrolled events on the Enterprise's business functions and processes.
- Classify the legal, financial, operational, reputational and regulatory risks for the Enterprise's business functions and processes.
- Determine the Maximum Allowable Downtime *("MAD")* associated with the Business Segment's processes.
- Establish the Recovery Time Objectives *("RTO")* and Recovery Point Objectives *("RPO"),* as appropriate for the dependencies associated with critical processes.

The BIA shall be reviewed and updated as needed on an annual basis and approved by the appropriate departmental managers.

Risk Assessment

The business continuity Risk Assessment is another step in the business continuity planning process. As such, the ABS Chief Technology Officer, Facilities Management and Bank Security in cooperation with the ABS BCM Leader shall initiate and maintain a risk assessment framework that focuses on physical risks to the workplace and site- based threat scenarios supporting ABS BCM Program.

- Evaluation of site risk.
- Analysis of site risk based on physical, environmental, natural and man-made threats.
- Prioritization of the physical risk impact based on severity and probability of occurrence.

The Risk Assessment shall be reviewed and updated as needed on an annual basis and approved by the appropriate departmental managers.

Business Continuity Plan and Recovery Strategies

This Policy requires that Business Segment Leaders develop or acquire the capabilities to execute BC recovery based upon the prioritized critical processes identified in the BIA and the risks defined in the Risk Assessment. Specific procedures for recovery of critical processes must be developed and documented in the BC Plans *(BCP)* such that employees understand their role in the recovery process and can implement the BCP(s) in a timely manner. The Enterprise BCM

Leader coordinates across the LOB Function and functions; identifies potential dependencies, including dependencies between various processes, IT applications, personnel, and suppliers *(including, but not limited to, external and internal suppliers);* and develops strategies to mitigate the risks related to interdependencies. External interdependencies are also recognized as potential points of failure and in those cases should be identified in the BCP *(e.g., telecommunication providers, customers & other business partners).*

The ABS BCM Leader must consider internal and external strategies to mitigate potential risks that have been defined. Specific mitigation strategies will depend upon the results of the BIA and the Risk Assessments, and will take into consideration other applicable risks*(such as supplier risk assessments pursuant to applicable Sourcing Policy and Procedures)*, and should ensure that processing priorities can be adequately implemented to address risks and that business operations can be resumed in a timely manner. The following list of "All Hazard" loss scenarios are considered as part of each mitigation strategy:

- Loss of workspace/facility.
- Reduction of workforce/specialized personnel.
- Loss of IT services.
- Loss of vendor services.

This plan should be reviewed and updated as needed on an annual basis or when significant changes occur. The department manager should review and sign off on the plan on an annual basis.

Test & Exercise Validation

Exercise validation is necessary to ensure that BCPs remain viable. A "BC Test Exercise" are planned or unplanned *(actual)* events whereby elements of a BCP are tested to rehearse steps, confirm responsibilities, and otherwise ensure that BCM capabilities are sufficient. The BCM Leader shall develop a BC Exercise framework that enhances the assurance for the continuity of critical business processes. This framework is used to develop a schedule of regular BC Exercises to demonstrate, evaluate and assess the effectiveness of the BCPs and the BCM Program. Results of the BC Exercises provide input for updates to BC Plans.

The following principles shall be addressed in the BC Exercise framework, regardless of who performs the BC Exercise:

- An exercise schedule is developed and BC Exercises are conducted at least annually, or more frequently, depending on changes in Apple Bank's operating environment or business criticality.
- The BIA and Risk Assessments serve as the foundation of the exercise schedule.
- Roles and responsibilities for implementation and evaluation of the BC Exercises are specifically defined.

- The breadth and depth of exercise activities are commensurate with the risk and importance of the business process to the Business Segment and/or to overall.
- BC Exercises are viewed as an evolution, starting simply and gradually increasing in complexity and scope.
- BC Exercise results are compared against the applicable BC Plans to identify gaps and weaknesses for remediation.
- Material issues identified through BC Exercises will be captured and tracked to resolution in BCM Post Test Report *(PTR)* and Action Tracking Dashboard.

Training

ABS's BCM Leader shall obtain and maintain certification in one of the key Business Continuity organizations: either Disaster Recovery Institute International *(DRII)* or the Business Continuity Institute *(BCI).* The BCM Leader issues awareness training for targeted populations to be completed annually. Business Segment Leaders are responsible for implementing additional training within their segments as required. Individuals in a recovery role shall participate in BC Exercises to support their responsibilities as part of the recovery team. This training should include the following:

- Business Continuity Overview for all staff
- Pandemic Training

Maintenance

The ABS BCM Leader reviews the BCM Program on an annual basis. Based on any changes in ABS risk, regulatory or compliance landscape, the BCM Leader will make the appropriate changes to Apple Banks BCM Program and Policy.

Business Segment Leaders ensure the maintenance of BC Plans. BC Plans are reviewed on an annual basis and upon significant changes to a process or upon gaps identified through an exercise or an actual event.

Policy Ownership and Approval

Ownership of the Policy resides with BCM Program Leader. The Technology and Operations Planning Committee (TOPC) and Operations and Technology Committee (OTC) of the Board review and approve the Policy periodically. The TOPC, OTC and the Board will also receive updates on the program annually.

The BCM Leader will oversee compliance with this Policy. Periodically, the Chief Technology Officer will update the TOPC and OTC on the health of the program which may include issues identified through exercises and actual events.

LOB Functions own their BC Plans, and therefore must document, implement, maintain & update specific business continuity procedures as required and/or needed in compliance with this policy. Additionally, LOB Functions will obtain approval of their BC Plans from the ABS BCM Program Leader on a regular basis.

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 ("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. 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. ABS staff will communicate their exception requests in writing to the Policy Owner, who will then present the request to the Designated Management Committee for consideration.

VII. 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.

VIII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for this Policy are summarized below:

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

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 an annual basis according to the Policy Level.

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 [Annual, Biennial, Triennial] basis according to the Policy Level (*refer to the Review and Tracking Chart*).

Executive Management Steering Committee (EMSC): To the extent necessary, the ESMC 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.

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.

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

Legal Contact: *See Section II – Definitions*.

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.

Chief Executive Officer ("CEO"): The CEO is ultimately responsible for and assumes ownership and leadership of the strategic planning process and ongoing reporting to the Board of Directors. The CEO establishes the "direction at the top" that affects integrity, ethics and other factors of the internal ABS environment. The CEO coordinates the process of aligning strategic planning with ABS's risk appetite and risk strategy and monitors the way senior management manages the businesses.

Chief Technology Officer ("CTO"): The CTO and his designated representatives are responsible for creating, reviewing new and updated procedures. The CTO is in charge of day-to-day oversight of Management policies and procedures.

Technology Operations and Planning Committee (TOPC): The Management committee reviews new and updated policies in order to advise on Encryption policy and procedures and to provide effective challenge of the proposed Encryption policies and procedures.

Operations and Technology Committee (OTC): The Board committee reviews new and updated policies in order to advise on Encryption policy and procedures and to provide effective challenge of the proposed Encryption policies and procedures.

Management and Business Units: The management and business units are responsible for ensuring compliance and understanding of this Policy as well as developing procedures that align with the requirements of this Policy. Management decisions must be consistent with this and all other approved ABS Policy and/or Procedure.

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.

BCM Leader: The person responsible for managing Apple Banks Business Continuity Program. Their responsibilities include overseeing Disaster Recovery testing, managing BC Plans, BC training, conducting the BIA and updating policies and procedures related to Business Continuity.

Department Manager: The person responsible for overseeing the functioning and productivity of a company division. Their primary responsibilities include recruiting and dismissing staff, establishing and working towards strategic departmental goals and managing a departmental budget.

Business Segment Leader: This is the departments designated person to oversee their Business Continuity responsibilities i.e. BC Plan, BIA, training.

IX. RECORD RETENTION

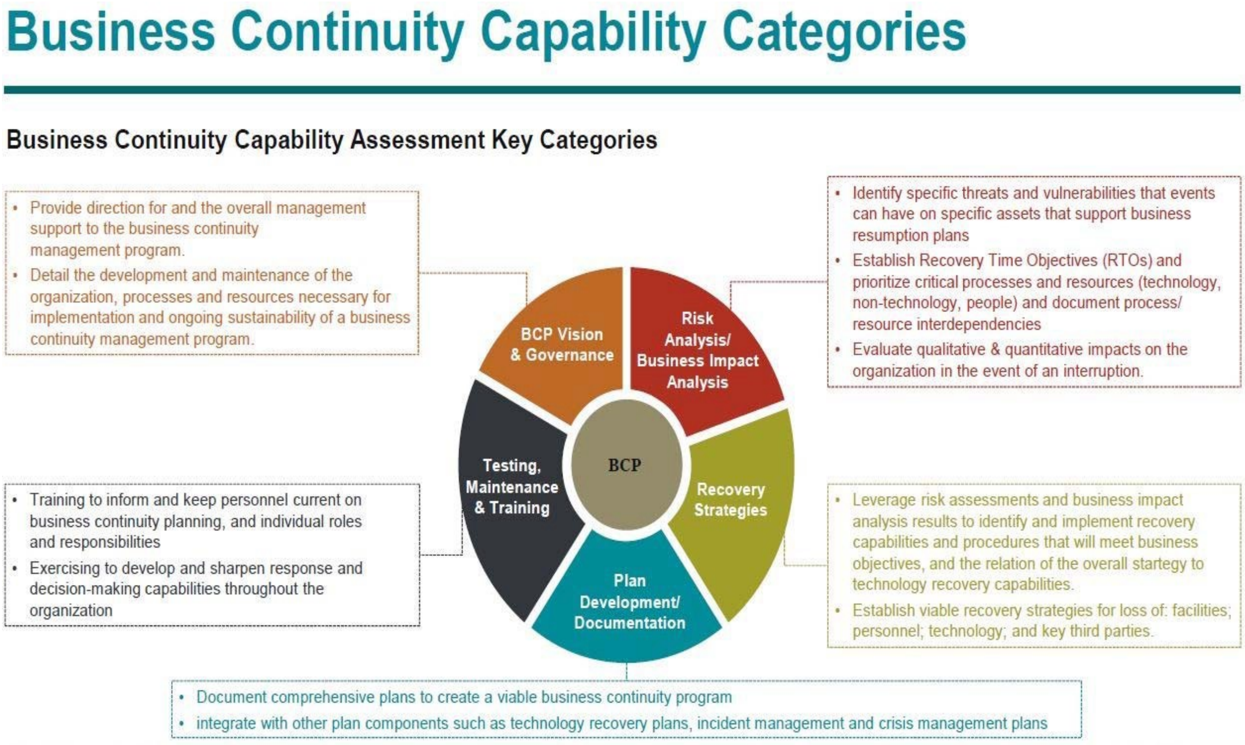
Any records created as a result of this Policy should be held for a period of 7 years pursuant to the Bank's Record Retention Policy. Should records created as a result of this Policy require a different retention period (either a shorter or longer time period), the Policy Owner (in conjunction with 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

APPENDIX “A” – BCM Components



Business Continuity Capability Categories

Business Continuity Capability Assessment Key Categories

BCP
BCP Vision & Governance
Risk Analysis/ Business Impact Analysis
Recovery Strategies
Plan Development/ Documentation
Testing, Maintenance & Training

- Provide direction for and the overall management support to the business continuity management program.
- Detail the development and maintenance of the organization, processes and resources necessary for implementation and ongoing sustainability of a business continuity management program.

- Identify specific threats and vulnerabilities that events can have on specific assets that support business resumption plans
- Establish Recovery Time Objectives (RTOs) and prioritize critical processes and resources (technology, non-technology, people) and document process/ resource interdependencies
- Evaluate qualitative & quantitative impacts on the organization in the event of an interruption.

- Training to inform and keep personnel current on business continuity planning, and individual roles and responsibilities
- Exercising to develop and sharpen response and decision-making capabilities throughout the organization

- Leverage risk assessments and business impact analysis results to identify and implement recovery capabilities and procedures that will meet business objectives, and the relation of the overall startegy to technology recovery capabilities.
- Establish viable recovery strategies for loss of: facilities; personnel; technology; and key third parties.

- Document comprehensive plans to create a viable business continuity program
- integrate with other plan components such as technology recovery plans, incident management and crisis management plans

APPENDIX “B” – Additional Roles and Responsibilities:

Business Leader (Each Business Segment / Line of Business (LOB))

- Appoint a Business Continuity Champion
- Ensure that competent and qualified personnel manage and are accountable for the processes necessary to ensure compliance with applicable policies.
- Integrate business continuity risk management and planning with business decisions.
- Oversee critical business processes and ensure that Business Continuity Plans are updated to reflect the current operating environment.
- Participate in the BIA process as owning a business process or group of processes.
- Approve BIA and Business Continuity Plans for business processes owned.
- Ensure process subject matter expert participation in test program planning, test results evaluation and gap or issue mitigation as required.

Business Continuity Management Leader ("BCM Leader")

- Ensure a comprehensive BCM Program is in place at Apple Bank, & in accordance with applicable policies that includes current:
- Business Impact Assessment ("BIA").
- Mitigation and Recovery Strategies.
- Business Continuity Plans for Apple Bank's defined critical processes.
- Ensure the implementation and maintenance of a comprehensive BCM Program in accordance with applicable policies.
- Review & recommend BCM Program approval to the TOPC and OTC annually.
- Maintain ultimate accountability for Apple Bank's BCM Program.
- Annual recovery test curriculum/schedule, program maintenance, and training.
- Governance, oversight and reporting of Apple Bank's business continuity preparedness metrics, test results, gaps, risks and issue resolution as required.
- Ensure BCM Program objectives and activities align with Apple Bank's leadership risk appetite, business recovery prioritization, and resource commitments.
- Ensure Business Continuity Plans are updated annually or when significant business process change occurs; are tested based on BIA and that test results, gaps and issues are reported as required.
- Coordinate with the Apple Bank's IT Disaster Recovery Leaders to appropriately integrate Business Continuity, Crisis Management and IT Disaster Recovery Plans and Programs, as required.
- Coordinate with Apple Bank's Vendor Management to evaluate the business continuity resilience of critical external suppliers as identified through the BIA and business continuity planning process.
- Coordinate with Apple Bank Business Leaders on internal and external communications in the event of an incident that threatens to or disrupts critical processes.
- Advise Apple Bank Leadership when need arises to activate Plans, as required.
  DR Program Leader ("IT Disaster Recovery Leader")
- Participate in the development and acknowledgement of business process impact analyses.
- Review IT recovery plans to support the business-critical processes as defined by the BIA, and evaluate capability to meet agreed RTO and RPO.
- Establish, maintain and track DR schedule to ensure DR plans are tested at least annually.
- Maintain IT Service recovery prioritization within Apple Bank.
- Coordinate DR tests and events with the BCM Leader as appropriate.

APPENDIX "C" – Documents Critical to Program

- Business Continuity Management Policy *(This Document).*
- Business Continuity Management BIA & Plans.
- BCM Test / Exercise Schedule.

- Vendor Risk Management Assessment Policy.
- Pandemic Plan

XIII. Revision History

Version	Date	Description of Change	Author	Approver
1.0	Feb 2018	Revised new format and enhanced for Business Continuity aspects, change reference to Apple Bank for Savings Business Continuity Plan, added Chief Technology Officer & Operations (CTO), and Disaster Recovery / Red Flag Identity Theft Administrator, removed Chief Administrative Officer, added reference to Data Center Disaster Recovery Manual, added Disaster Recovery, Crisis Management, Cybersecurity events, or other to Risk Management, added Crisis Management team to document	William Di Pinto Technology, A.T., Disaster Recovery / Business Continuity / Red Flag Identity Theft / GLBA / Incident Response Administrator	Board
2.0	April 2019	Enhanced for Business Continuity aspects, change reference to Apple Bank for Savings to Apple Bank Business Continuity Plan, added Assessment Team, IT Recovery Team, Site Restoration Team, and Support Services Team to document	William Di Pinto Technology, A.T., Disaster Recovery / Business Continuity / Red Flag Identity Theft / GLBA / Incident Response Administrator	Board, Operations and Technology Committee
3.0	May 2020	• Update template • Added definitions	Anthony Scarola, FVP	Board, Operations and Technology Committee
4.0	May 2021	Updated the Policy using the current Policy Template (February 2021). Enhanced for Business Continuity aspects, including: • Modify the Executive Summary • Add frequency of BC Plan and BIA review and approval • Added and updated definition to be more in line with industry standards • Add critical program documents	David James, VP Sean Friedman, AVP	Board, Operations and Technology Committee