Apple Financial Holdings, Inc.

IT Risk and Control Self-Assessment ("RCSA") Procedures

MAY 2021

Contents

REVIEW AND TRACKING CHART

Effective Date:	May 2021
Version Number:	1.0
Review Frequency:	Annually
Last Business Area Leader Review Date:	N/A
Next Business Area Leader Review Date:	May 2022
Business Area Leader or Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	Information Security Policy, Risk Management Framework Policy, Operational Risk Management Policy
IT RCSA Procedures Owner:	IT GRC-CM IT Risk Control Officer, Technology Department

*The review and effective dates above should only be updated after the appropriate meeting where the review or approval occurs. Prior to such meeting the dates should reflect the "old" dates of review. For clarity, do not use anticipated/prospective dates for Last Review or Effective dates.

I. PURPOSE STATEMENT AND SCOPE

The Information Technology Risk and Control Self-Assessment ("RCSA") Procedures (the "Procedures" or the "IT RCSA procedures") applies to the implementation, management, monitoring and completion of the RCSA process as part of the first line Operational Risk Management ('ORM") at Apple Bank for Savings and its subsidiaries (collectively, "ABS", "Apple", or the "Bank") in accordance with the 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 the IT RCSA procedures to the degree applicable to them.

II. DEFINITIONS

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

- **Control Effectiveness**: Design and operating effectiveness of the active control in place to mitigate a particular risk.

- **Business Area Leader or Department Head:** The lead of a business area or a department who is responsible for the implementation of the controls and associated processes.

- **Self-Identified Issues ("SII"):** Deficiencies or weaknesses in the current control environment that are self-identified by the process owner and recorded in GRC.
- **IT RCSA Assessor**: The individual(s) responsible for the execution of the IT RCSA process.

- **Inherent Risk**: The potential risk in place before relevant actions are taken (i.e., before relevant controls are implemented to alter/mitigate the risk's impact or likelihood).

- **Residual Risk**: Risk remaining after the entity's response to the Inherent Risk (i.e., after the application of controls and control processes to manage inherent risk).

- **Procedures Owner:** The person responsible for managing and tracking a set of Procedures. This includes initiating the required Annual review of the relevant Procedures and recommending updates to the Procedures, to the extent needed. Procedures Owners are responsible for providing the approved documents to the PPA (defined in this Section) for upload to AppleNet, as necessary. The Procedures Owner will monitor these Procedures. Any non-compliance with the Procedures will be escalated to the Business Area Leader or Department Head for resolution. If the issue cannot be resolved by the Business Area Leader or Department Head the issue will be escalated to the Designated Management Committee for resolution.

III. IT RCSA PROCEDURES

1. EXECUTIVE SUMMARY

This document outlines ABS's procedures to execute an IT Risk and Control Self-Assessment ("IT RCSA") for the First Line in accordance with Risk Management's *Risk Management Framework Policy* and *Operational Risk Management Policy.*

The goal of the IT RCSA procedures is to establish a standardized and consistent approach to the

executing of IT RCSA for specific process areas. The IT RCSA procedures will be designed to identify all potential control deficiencies and to facilitate their remediation in a timely manner.

2. OBJECTIVES

The primary objective of the IT RCSA is to determine that appropriate controls are in place, and that the design and operation of the controls are effective in mitigating the inherent risks of the critical Information Technology processes. The appropriate controls can be detective or preventive, manual or automated.

While the bank-wide annual RCSA program will encompass all key functional areas, specific RCSA procedures may be designed to apply to specific business and technology areas in the bank.

As part of the process all interested parties, Internal Audit, 2nd line, Info Security, business and process owners will be invited to all the Roundtable meeting and discussions concerning the RCSA processes.

The IT RCSA is the process by which ABS Information Technology's personnel collectively identify and evaluate risks and associated controls of key business lines and processes. The IT RCSA procedures are updated and executed across the bank's key business units and processes on an annual basis, or more frequently if necessary RCSA processes and results are owned by the relevant process owners (First Line), and are reviewed by Operational Risk Management (Second Line) and Internal Audit (Third Line).

3. KEY PROCESS COMPONENTS

The completion of the Information Technology RCSA involves a number of steps which are outlined in the RCSA Operational Risk Management Procedures. What follows provides additional supplemental detail.

Core components of the RCSA process include, but are not limited to: key process and steps, key risks and controls, ratings for impact and probability, inherent risk, control design and effectiveness, control rating and residual risk.

ABS has implemented a GRC tool, which will be used to support and document the RCSA. Please see – GRC User Manual on AppleNet for details .

Step 1 - Identification of In- Scope - Key Systems/Processes

The Assessor must determine the in-scope assets and domains, as well as the key core processes. This will involve the participation of key stake holders, ORM, CTO and will include the critical examination of past IT RCSAs for guidance.

Once the initial identification has been completed, a presentation deck and relevant information will be provided to each of the areas under review. The presentation deck will outline among other topics, the scope, timing, and requests for documentation etc. Please see Appendix 1 for a sample of presentation, which can be used to kick off the annual RCSA process.

Step 2 - Identification of Key and Non-Key Controls for Assessment and Testing

Discussions will be held with each IT business/process owner to gain an understanding of the relevant control environment. As part of the discussion, key and non-key controls will be identified and documented.

Step 3 - Determining the Inherent Risks

Discussions will be held to determine the inherent risks of each one of the controls under review.

Step 4 - Testing and Assessing Control's Design and Operating Effectiveness

Based on the controls identified in Step 1, an evaluation will be performed over the design of the controls. Should the design of the control be assessed effective, testing will be performed to assess the operating effectiveness of the control.

Please see the next section in the RSCA Execution for further details

IV. RCSA EXECUTION

The IT RCSA will be broken down into several areas, which can be executed sequentially or in parallel, depending on the processes. Please see Exhibit II for a high level work flow of the IT RCSA process.

(Note: The steps outlined here are generalizations that can be changed based on the risk encountered and other operational characteristics.)

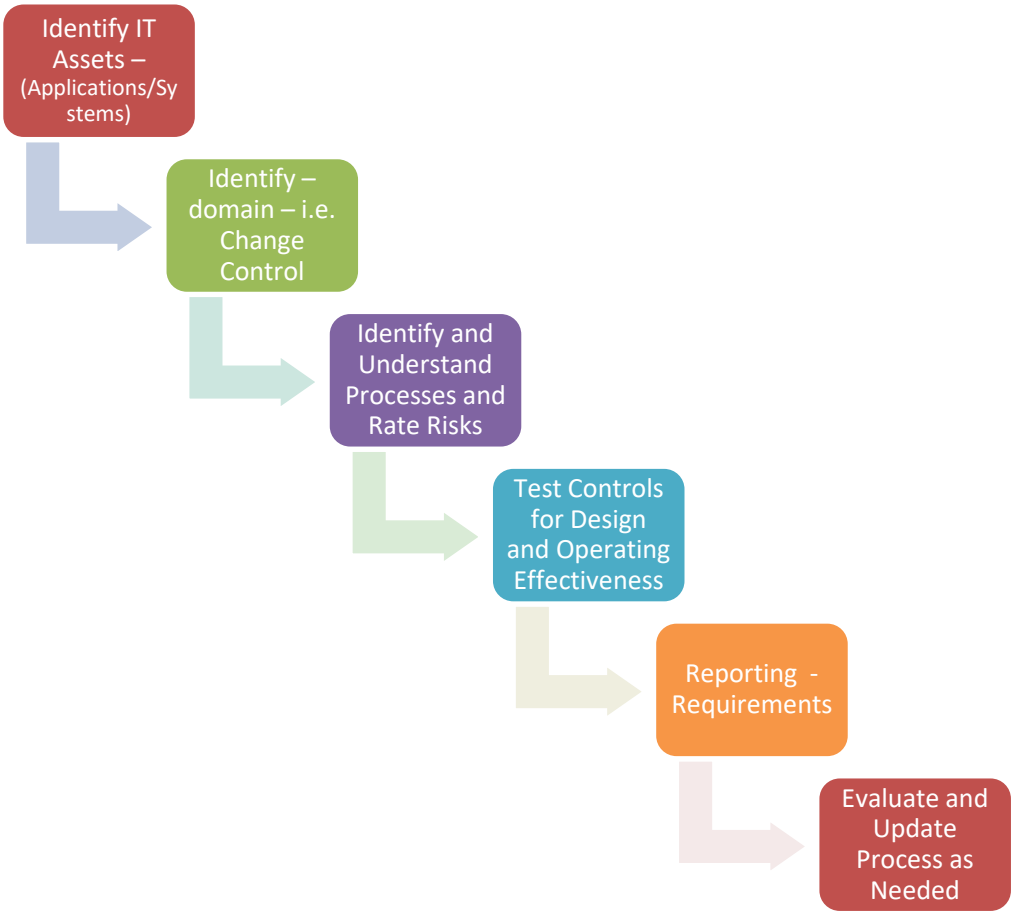


Exhibit II
RCSA Work Flow

Step 1 - Scoping - Identifying IT Assets and Domains

At the start of the year or of a review period that the RCSA will cover, the in-scope processes and their related entities will be determined. All current information assets such as end-user applications, software and hardware will be identified in this step.

Discussion will be held with all process owners and stakeholders, to include items such as: IT Operations, Change Control Process and Identity Access Management, etc.

The in-scope RCSA areas may include:

- Encryption
- Data Classification
- IT Security
- IT Strategy and Governance
- IT Development and Acquisition
- IT Operations
- Change Management
- IT Infrastructure
- Business Continuity Planning

- Electronic Banking

Once the in-scope areas have been identified, a meeting will be held with ORM, IT Operations and Information Security to obtain their approval of the scope.

Step 2 - Planning

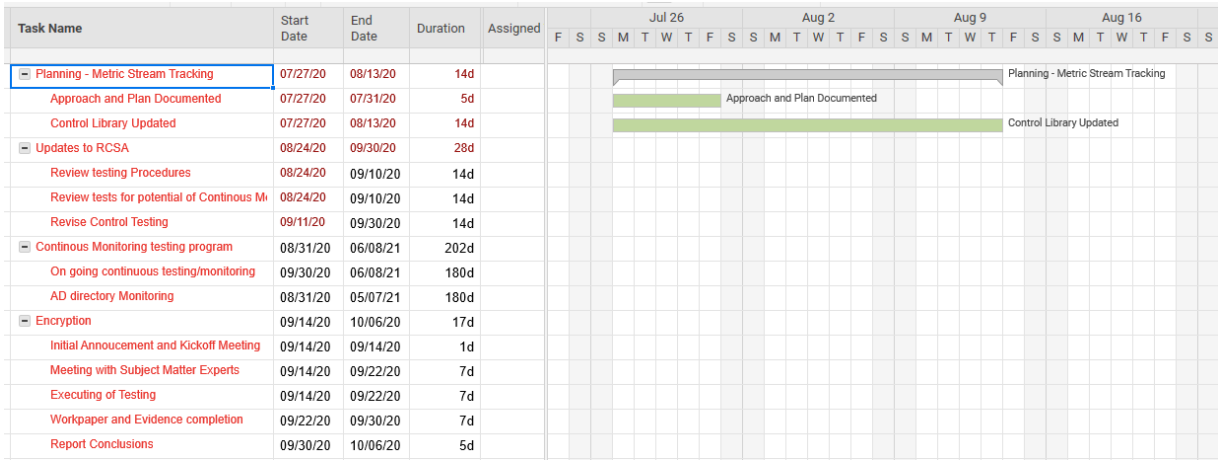
After the scoping is complete, the execution of the RCSA will be scheduled. Tools such as ZOHO, MS Project or Excel spreadsheets can be used. Once developed, the preliminary time line will be reviewed with the process owner(s) to obtain buy-in and support.

A schedule will be proposed for each in-scope area. Please see the example of a typical time Line:

- Planning – 2 weeks
- IT Security – 8 weeks
- IT Strategy and Governance – 3 week
- IT Development and Acquisition – 4 weeks
- IT Operations - 3 weeks
- Change Management – 3 weeks
- IT Infrastructure – 8 weeks
- Business Continuity Planning – 2 weeks
- Close out – 2 Weeks.
- QA review by second line – 4 weeks

The final working schedule shall take inputs from relevant stakeholders, including the second line / ORM and Information Security, to address any possible conflicts or overlaps. .

Once the scoping and timing are finalized, a memo or email will be sent to all applicable stakeholders to publish the scope and timing of the RCSA. Stakeholders will include at a minimum: business process owner, and executive in charge/responsible for the area such as the CTO and Head of ORM. Other optional stakeholders could include other business areas such as Internal Audit. See Exhibit III for a sample of RCSA project plan.



Task Name	Start Date	End Date	Duration	Assigned
Planning - Metric Stream Tracking	07/27/20	08/13/20	14d	
Approach and Plan Documented	07/27/20	07/31/20	5d	
Control Library Updated	07/27/20	08/13/20	14d	
Updates to RCSA	08/24/20	09/30/20	28d	
Review testing Procedures	08/24/20	09/10/20	14d	
Review tests for potential of Continous M	08/24/20	09/10/20	14d	
Revise Control Testing	09/11/20	09/30/20	14d	
Continous Monitoring testing program	08/31/20	06/08/21	202d	
On going continuous testing/monitoring	09/30/20	06/08/21	180d	
AD directory Monitoring	08/31/20	05/07/21	180d	
Encryption	09/14/20	10/06/20	17d	
Initial Annoucement and Kickoff Meeting	09/14/20	09/14/20	1d	
Meeting with Subject Matter Experts	09/14/20	09/22/20	7d	
Executing of Testing	09/14/20	09/22/20	7d	
Workpaper and Evidence completion	09/22/20	09/30/20	7d	
Report Conclusions	09/30/20	10/06/20	5d	

Exhibit III
Sample RCSA Project Plan

Step 3 – Understanding the Key Processes and Applicable Controls

In this step, the assessor will schedule meetings with the key process owners. In this meeting (and possible follow-up meetings), the following topics will be discussed and confirmed:

A. Review RCSA results of previous year. This review's objective is to gain an understanding of the previous year's assessment and testing. The following areas will be covered, at a minimum:

- Status of outstanding control failures/deficiencies: Updates on the current status and remediation plans;
- Self-Identified Issues: detailed description, potential risks, current status and remediation plans;
- Issues identified by the Internal and External Auditors per end of last RCSA review: Follow up on current status and remediation plans;
- Changes in control wording in view of changes in control process, ownership/control operation and underlying technology; and,
- New or updates of documentation of Processes under discussion.

B. Discussion of the process under review (e.g., change control), including an examination of the supporting documentation, such as operating manuals and/or procedures both written and informal (unwritten).

C. Discussions of the underlying Risk within the Process. Topics discussed should include:

- Threats and Vulnerabilities;
- Related risk information: scope, nature, stakeholder, quantification, risk tolerance/appetite, etc.
- Controls and procedures that are currently and/or will be in place to mitigate the risk; and,
- Any relevant Compensating Controls.

Documentation of Understanding

Wherever applicable, the understanding of the control (process, ownership/operation personnel, and underlying technology) will be documented, at a minimum, both in written narratives and flowcharts.

All the above information will be documented in a controls matrix. A completed template is available in the shared folder "\\BR216Fs1\Risk Control Self- Assessment\ RCSA Templates".

All finalized documentation will be saved and maintained in GRC. Please see the GRC User Manual on AppleNet for further details.

Step 4 - Test the Controls Design and Operating effectiveness

The testing of IT RCSA will follow the generic process of as Outline in Risk and Control Self-Assessment Procedures document, which is depicted in the flowchart below:

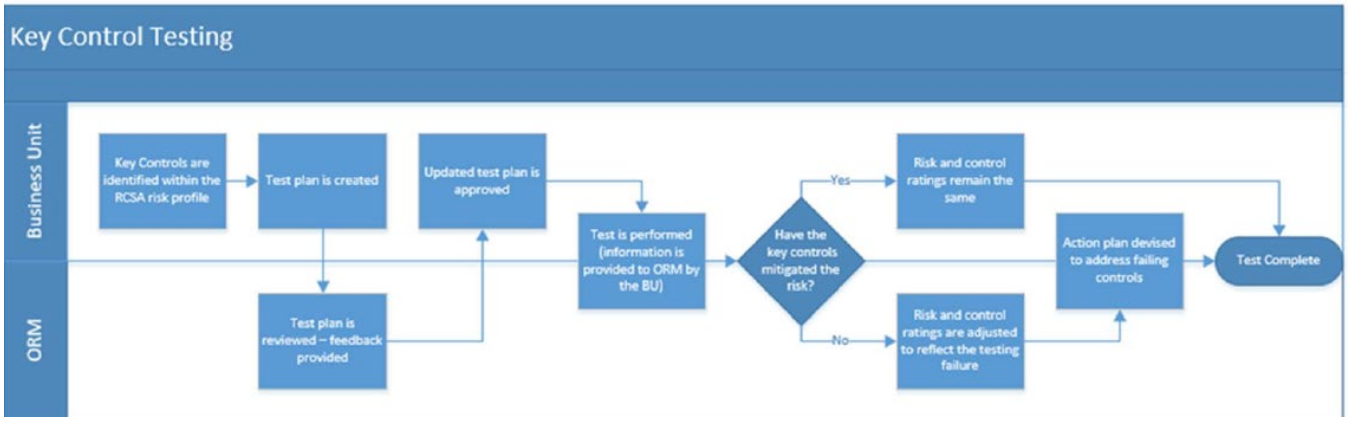


Fig. 2 Key Control Testing Flowchart (Ref. "Risk and Control Self-Assessment Procedure"

Testing of Design Effectiveness

The test of design of an internal control validates that a control, stated to be in place to mitigate a specific risk, has indeed been established and active at least at the RCSA review time.

To determine whether the design is effective, the reviewer will select a sample of one to perform a walkthrough based on the understanding of the related risk, the related business/IT process and the control's attributes (the control's process, people and technology).

If the reviewer confirms that the sample is representative of the control process and that the identified risk can be appropriately mitigated, then the design of the control can be assessed as effective.

To illustrate the above we use the change management process. As part of our example the control description specified that all changes to the bank's information assets must be authorized through appropriate reviews and subsequently tested prior to implementation.
Consequently, the reviewer testing the design of these change management controls would validate that, based on the evidence from a sample of one, the following actually occurred:

- the change was appropriately reviewed (typically by peers)
- the change was appropriately tested (typically automated testing and human testing)
- the change was approved by appropriate personnel

If the information outlined above is available for the change sample, the RCSA reviewer would be able to confirm that the internal control process for change management was in place and its design effective.

Testing of Operating Effectiveness

The test of operating effectiveness is to confirm that a control, whose design has been assessed effective, is operating so that the related risks are mitigated as per the control's intent during the assessed period.

In the change management example from the previous paragraph, the reviewer will test the operating effectiveness by sample testing.

This requires the RCSA reviewer to obtain a population (e.g. a complete listing) of all of the system changes that have occurred during the audit window (typically a 12 month-period, if this is an annual test).

The reviewer would then select a sample of changes from the above population. The sample size is determined as described below. The sample will be selected either at random or through professional judgment. For each selected sample of change, the reviewer would look to confirm whether all the control's attributes, including peer review, testing, and approvals, are successfully completed before the change was considered as completed.

Determining Sample Size

1. **Automated Controls** – For automated controls, one sample per automated control is often required for up to a period of 3 years. This is based on the assumption that an automated control will perform effectively, unless there were changes within the 3-year period that impacted the effectiveness of its operation. The other assumption is that the inner details of the automated controls are available for the reviewer to assess. If "white" box testing was not possible, the reviewer may classify the automated control as "manual", and therefore tested as such.

   Examples of automated controls include:

   - Automatic lock out of an account consequent to excessive number of log-in attempts
   - Automatic disabling of single-sign-on and access to ABS's information assets in the absence of ABS' VPN
   - Automated ("hands-off") creation of a key report

2. **Manual Controls** – For manual controls, the annual sample size will depend on the control frequency. The table (from "Risk and Control Self-Assessment Procedure ") below provides the sampling guidelines for manual control testing:

Table 1. Minimum Sample Size per Control Frequency (Ref. "Risk and Control Self-Assessment Procedure" (OPRISK))

Control Frequency	Minimum Sample Size
Annual	1
Quarterly	2
Monthly	3
Weekly	5
Daily	20
Transactional (Ad hoc)	At testing manager's discretion

Should exceptions be found during the testing, additional samples may be selected in order to assess whether the control is deficient (or not). A guidance on the required additional sample size is provided below. Note that the sample size is a function of the control rating and the number of samples that was used in the prior testing.

Table 2. Additional Test Sample Size in case of Exceptions

Number of Control Testing Exceptions		Control Rating
< 10 samples	> 10 samples	
0	1	Strong
1	2	Adequate
2	3 or more	Weak

Additional samples may be required at the reviewer's discretion, depending on the results of the initial test or other applicable circumstances (e.g., changes in risk rating, changes in control scope.).

The above sampling guidelines apply to controls that are not tested by the first line but by the second line of defense.

Frequency of Control Testing

The RCSA scope of control testing is based on established criteria. These are mainly driven by the inherent risks of the underlying processes and business activities.

The RCSA program aims to test most key controls on an annual basis. The testing frequency for all controls is described below:

- Annual Testing
  - An RCSA with a "Very High" or "High" inherent risk
  - Any changes to a key control which are deemed critical to the process
- Two Year Testing
  - An RCSA with a "Moderate" inherent risk.
- Three Year Testing
  - An RCSA with a "Low" inherent risk

Note that the actual testing frequency of the control is left at the reviewer's discretion. The above guidance is in line with the procedures in "Risk and Control Self-Assessment Procedure".

Residual Risk

A residual risk value will be determined and calculated for each control.

INHERENT RISK – CONTROLS = RESIDUAL RISK

The control rating is applied to the inherent Risk Rating to come up with a Residual Risk Rating. This rating is based on the below. This table is part of the ORM Methodology.

Residual Risk Rating

Control	Low	Moderate	High	Very High
Weak	Low	Moderate	High	Very High
Adequate	Low	Low	Moderate	High
Strong	Low	Low	Moderate	Moderate

Inherent Risk

Reporting

The reviewer will report all the observations, so that they can be vetted by the process owner for accuracy. Once accepted, the observation will become an issue, whose resolution needs be agreed upon.

A summary report will be generated at the conclusion of each section of the IT RCSA with the

appropriate finding/recommendations and residual risk ratings.

Control "gaps" will be identified and documented, along with the remediation plans (developed in conjunction with the business/process owners, Information Security and/or IT Risk Management as appropriate). This includes any issues identified during the RCSA workshops. An issue will be entered into GRC for any new finding identified.

A final summary report covering the entire IT RCSA program will be generated at the conclusion of the yearly RCSA program.

Documentation of Work

Step 5 – Documentation of RCSA Work

All IT RCSA assessments and tests will be documented to support the final conclusions. Included in the relevant documentation are diagrams, meeting notes, screen shots, etc. This documentation will be made available to Risk Management, Information Security, external and internal auditors as well as regulators as required.

All work will be documented in the Metric Stream GRC Package. Please see the IT RCSA Procedures Manual for detailed instructions.

Step 6 – Review of IT RCSA

The completed IT RCSA will be reviewed by the second line or designated proxy and/or Internal Audit as required. All supporting documentation and work will be made available on request

V. REQUIRED ANNUAL (12 MONTH) REVIEW

Procedures are required to be reviewed and approved at least Annually by the Business Area Leader or Department Head. The Procedures Owner is responsible for initiating an Annual review of the Procedures. The Procedures Owner will track the review date for the Procedures and begin the review process early enough to provide ample time for the appropriate review to occur in a timely manner.

Once updated Procedures have been approved by the Business Area Leader or Department Head , the updated Procedures shall go into effect and the Procedures Owner shall be responsible for delivering the approved Procedures together with a Control Form 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 Procedures are stored and made available to the employees of the Bank.

The Next Business Area Leader/Department Head Review Date shall be adjusted accordingly.

VI. OFF-CYCLE REVIEW AND APPROVAL PROCESS

If the Procedures require changes to be made outside the Required Annual (12 Month) Review outlined in the previous section, the same steps as outlined in the previous section shall apply.

VII. EXCEPTIONS TO THE IT RCSA PROCEDURES

Requests for exceptions to these Procedures must be specific and may only be granted on specific items, rather than to entire sections. ABS/AFH staff must communicate their exception requests in writing to the Procedures Owner, who will then present the request to the Business Area Leader or Department Head for consideration.

VIII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for these IT RCSA procedures are summarized below:

Business Area Leader: *See Section II – Definitions*.

Server Infrastructure: Provide IT Response to all Active Directory Events questioned by IT/ IS Operations.

Information Security Operations: IT / Information Security Operations is responsible for reviewing the Active Directory events logs and identifying any questionable activities performed by the IT Department.

Policies and Procedures Administrator ("PPA"): The PPA is a member of Risk Management, and in charge of uploading the approved policies, procedures, and manuals onto APPLENET.

IT RCSA Procedures Owner: The owner is responsible for managing and tracking the IT RCSA procedures. This includes initiating the required Annual review of the relevant IT RCSA procedures as well as recommending updates to the procedures, to the extent needed. The IT RCSA Procedures Owner is responsible for providing the approved documents to the PPA (defined in this Section) for upload to APPLENET. The IT RCSA Procedure Owner is responsible for the monitoring of the IT RCSA procedures. Any non-compliance will be escalated to the Business Area Leader or Department Head for resolution.

IX. RECORD RETENTION

Pursuant to the ABS's Record Retention Policy, records that are created as a result of the RCSA program will be held for a period of 7 years. All exceptions (e.g. records to be retained for either a shorter or longer time period) need be submitted with the supporting rationale by the IT RCSA Procedures Owner to the Business Area Leader or Department Head. Upon approval, the resulting deviation from the record retention policy and its supporting rationale will be accordingly recorded and therefore available to any possible inquiries.

Any records created as a result of these Procedures should be held for a period of 7 years pursuant to the Bank's Record Retention Policy. Should records created as a result of these Procedures require a

different retention period (either a shorter or longer time period), the Procedures Owner must describe the rationale for a different retention period and share the rationale with the Business Area Leader or Department Head, who shall in turn document the deviation and supporting rationale in such a way that it can be presented to relevant parties upon request.

XII. QUESTIONS AND CONTACT INFORMATION

Questions regarding to the compliance with the IT RCSA Procedures may be addressed to the IT RCSA Procedures Owner, as listed in the tracking chart on the first page of this document.

XIII. LIST OF REFERENCE DOCUMENTS

1. *Risk Management Framework Policy*
2. *Operational Risk Management Policy*

XIV. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.0	May 2021	New Procedure	Allen Lum VP of Compliance	