Apple Financial Holdings, Inc.

Business Application Service Catalog Management Procedure

November 2021

Contents

PROCEDURES NAME: Business Application Service Catalog Management Procedure

REVIEW AND TRACKING CHART

Effective Date*:	November 2021
Version Number:	1.6
Review Frequency:	Annual (Every 12 Months)
Last Business Area Leader/Department Head Review Date*:	November 2021
Next Business Area Leader/Department Head Review Date*:	November 2022
Business Area Leader/Department Head:	Debi Gupta, CTO
Overarching Policy or Policies:	AFH IT Asset Management Policy AFH Data Governance Policy
Procedures Owner:	Anthony Scarola, FVP Technology, IT GRC-CM

I. PROCEDURES PURPOSE STATEMENT AND SCOPE

The Business Application Service Catalog Management Procedure (the "Procedures") apply to the management of business application services assets (a.k.a., "software") in compliance with the AFH IT Asset Management Policy] 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 these Procedures to the degree applicable to them.

II. DEFINITIONS

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

- **Business Area Leader or Department Head:** The management level person who is responsible for (1) the business unit that has developed a set of Procedures and (2) the Annual review and approval of Procedures.

- **Control Form:** The form to be submitted to the PPA (defined in this Section) in connection with revised Procedures. The Control Form is available on AppleNet.

- **Legal Contact:** The attorney from the Legal Department assigned to the group responsible for these Procedures. To the extent needed, the Procedures Owner may consult with the Legal Contact in drafting and updating the Procedures.

- **Policies and Procedures Administrator ("PPA"):** The PPA is a member of Risk Management. The PPA monitors the occurrence and timeliness of scheduled Procedure reviews, obtains updated versions of Procedures, and ensures that they are uploaded to AppleNet within seven days of the approval dates of the documents.. The PPA will also provide guidance on the PPGP (defined in this Section) to Bank Personnel.

- **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.

- **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.

- **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. 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.

III. KEY PROCEDURES COMPONENTS

1. Executive Summary

This document outlines AFH's Procedures with respect to the management of the Business Application Service Catalog to include the cataloging of business applications and their comprising application services assets (a.k.a., "software") in compliance with the *IT Asset Management Policy*.

2. Objectives

The objective of these Procedures is to establish a standardized and consistent approach to managing the AFH business application service assets.

3. Key Components of Procedures

A. Catalog System and Sensitivity

The Business and Application Service catalog is stored within the Bank's ServiceNow Application Portfolio Management (APM) repository.

The catalog is classified as "Restricted data" per the Information Security Data Classification Policy. If access to the Software Inventory is required, request such access via management. IT GRC-CM Manager will provide access approval based on business need.

B. Business Application Service Catalog Data

The business application services catalog includes the data fields outlined and described in Appendix A.

C. Catalog Update Process

On a semi-annual basis, or more frequently as needed, the IT GRC-CM team will acquire data from the following sources in an effort to update and keep current the catalog:

- Vendor Management Database
- IT Strategic Plan, TOPC and NPIC Meeting Minutes
- Business Line Application/Services Owners

The process for acquiring this information from the sources above is as follows:

- Vendor Management Database

  The Risk Management/Vendor Management department maintains a listing of application vendors to include those with which the Bank acquires licensed software. Semi-annually, this list must be acquired and reviewed/compared against to ensure the Software Inventory is accurate.

- IT Strategic Plan, TOPC and NPIC Meeting Minutes

  The IT Strategic Plan, Technology & Operations Planning Committee (TOPC) and New Products and Initiatives Sub-Committee (NPIC) meeting minutes should be obtained from the Office of the CTO. These three sources should be used to identify any new or soon-to-be-implemented licensed software assets to ensure they are captured within the Software Inventory.

- Business Line Application/Services Owners

  Every licensed application asset is "owned" by a department-level/business line representative. This individual is the "Application Owner" and/or "Data Owner" and is responsible for ensuring accurate information is cataloged for their licensed application service assets. Quarterly, representatives from the business lines will be provided with their respective current application catalog so that they may review and update it. The IT GRC-CM team facilitates this update and may do so via email or via meeting. The business line representatives will be provided two to three weeks to complete the update task. Updates will be captured within the catalog by the IT GRC-CM team.

4. Escalation Procedures

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.

IV. 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.

V. 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.

VI. EXCEPTIONS TO THE PROCEDURES

Requests for exceptions to these Procedures must be specific and may only be granted on specific

items, rather than to entire sections. ABS 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.

VII. ROLES AND RESPONSIBILITIES

The key roles and responsibilities for these Procedures are summarized below:

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

Business Area Leader or Department Head: *See Section II – Definitions*.

Internal Audit: The Internal Audit team is responsible for the periodic audit of these Procedures. 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*.

PPA: *See Section II – Definitions*.

Procedures Owner: *See Section II – Definitions*.

Senior Management: Members of management and business units are responsible for developing and implementing these Procedures which align with the requirements of the overarching Policy or Policies to which these Procedures relate, and ensuring compliance and understanding of these Procedures.

VIII. RECORD RETENTION

Any records created as a result of these Procedures should be held pursuant to the Bank's Record Retention and Disposal 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.

IX. QUESTIONS AND CONTACT INFORMATION

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

X. LIST OF REFERENCE DOCUMENTS

- Data Governance Policy

- IT Asset Management Policy
- Record Retention and Disposal Policy

XI. REVISION HISTORY

Version	Date	Description of Change	Author	Approver
1.6	11/2021	Updated to reflect changes with the IT Operating Model. Merged with the new Procedure Template.	A. Scarola	Debi Gupta, CTO
1.5	6/2021	Update to reflect changes with the cataloging process, ServiceNow tool use, Data Governance requirements and data field names. Renamed document to reflect ITIL and ServiceNow terminology.	A. Scarola	Debi Gupta, CTO
1.0	10/2020	New document.	A. Scarola	Debi Gupta, CTO

Appendix A – Business Application Service Catalog Data Fields and Definitions

1. **Number**
   A unique identifier, defined by ServiceNow. Cannot be changed.

2. **ID**
   A unique identifier, historically defined by the IT GRC-CM team.

3. **Vendor**
   The vendor/developer's name. For example, "Google", "Microsoft" or "FIS". For applications developed by the Bank (e.g., AppleNet intranet website), use "ABS". Note, vendors are entered into a separate data store within ServiceNow.

4. **Vendor ID**
   Link to the Vendor database. Automatically generated by ServiceNow. Cannot be changed.

5. **CMDB Major ID**
   Link to the ServiceNow CMDB software database. Entered by IT GRC-CM team if the data is available.

6. **Name**
   The application service name. For example, "MISER". For a website/web portal, use the website/web portal's name (e.g., "Gmail").

7. **Description**
   Enter a brief description of the application service (i.e., the software) and what it is used for.

8. **Version**
   The version number or release name of the application service, if applicable. For example, "2.5", "2019" or "Orlando". If unsure/unaware, contact the vendor for details. Note, some online services may not have a version number.

9. **Operational Status**
   Used to identify the current operational status of the application service. Typical values are "Operational", "Sunset", and "Planned"; however, other options are available.

10. **Business Need**
    Answer the question(s), "Why does the Bank need this application service?" and "What function does the service provide to the business?" For example, "transacting business (opening/maintaining accounts and assisting customers", "record purchases, payments and income", "prevent the Bank from violating a law/regulation", "securities and cash movement", "protect sensitive data", etc. Be general but detailed enough for others outside of your business line to understand.

11. **Business Application**
    The higher-level business application name. Current values are below (match to the nearest value or enter a new one as needed):

- Account Origination
- Account Reconciliation
- Accounting
- Accounting - Account Reconciliation
- Accounting - Accounts Payable
- ACH File Transmission
- ACH Posting & Returns
- Appraisal Management
- Asset & Document Verification
- Asset Management
- ATM Driving and Card Management
- ATM/DBT Card Inventory Management
- Audit Management
- Banking - Fraud Detection
- Board Management
- Board Management - Collaboration
- Branch Check Capture
- Branch Currency Ordering
- BSA/AML
- Business & Consumer Credit Card Application Management
- Business and Consumer Direct Mail Campaign Approval
- Business Prospecting
- Card Production and Invoice Management
- Cash Flow Analysis
- Cash Management
- Certificate of Deposit Account Registry Service Management
- Chargebacks - Return Check Credits
- Check Ordering
- Check Processing
- Commercial Loan Servicing - Remittance Reports
- Commercial Mortgage Servicing
- Commercial Mortgage-Backed Securities Analysis
- Company Internal Website
- Compliance Management
- Construction and Property Inventory
- Construction Cost Estimating
- Consumer Complaints
- Core Banking - Infrastructure
- Core Banking - Mainframe Access
- Core Banking - Mainframe Security
- Core Banking - Mainframe Utility
- Core Banking System
- Corp Real Estate Billing
- Counterfeit Note Searching

- Credit Management
- Currency Delivery Customer Support and Management
- Currency Transactions Management
- Customer Account Reconciliation
- Customer Identity Verification
- Customer Line Call Recording
- Customer Voice Response System
- Data Backup
- Data Warehouse
- Debit Card Processing Service
- Development Source Control and Change Management
- Direct Mail Campaigns
- Disaster Recovery / Business Continuity
- Document Imaging and Printing
- Document Management - Cold Storage
- Document Storage and Retrieval
- Document Storage and Retrieval / Processing
- Electronic Check Processing
- Employee Benefits Management
- Employee Collaboration
- Employee Employment Verification
- Employee General Training
- Employee Identification
- Employee Insurance Management
- Employee Organizational Charting
- Employee Payroll
- Employee Pension Management
- Employee Recruiting
- Employee Remote Access
- Employee Retirement Funds Management
- Employee Survey Administration
- Employee Time Management
- Employee Training
- Employee Unemployment Claims
- Employment Applicant Tracking
- Employment Background Checking
- Ethics Complaint Management
- Financial Reporting and Budgeting
- FIS Vendor Product Management
- Foreign Check Collection
- Foreign Currency Exchange
- Fraud Detection
- High Risk Check Order Resolution
- HMDA Loans Tracking and reporting

- Image License Management
- Insurance and Annuities Management
- Interest On Lawyer Account (IOLA) Deposit Management
- International Wires
- Internet Access
- Investment Management
- Investment Portfolio Management
- Investment Securities Pricing
- Large Dollar Return Notifications
- Lease Accounting
- Loan Guarantee Registration
- Loan Origination
- Long Term Disability Insurance
- Merchant Services Referral Submission and Reporting
- Money Movement
- Mortgage Loan Servicing
- Name Screening
- Network Activity Auditing
- Network Infrastructure
- Network Security - Auditing
- Network Security - Cloud Protection
- Network Security - Communication Protection
- Network Security - Data Protection
- Network Security - Employee Training
- Network Security - Endpoint Protection
- Network Security - Incident and Event Management
- Network Security - Network Protection
- Network Security - User Authentication
- New York Tax Match
- New York Tax Match - Child Support Collection
- Online Banking
- Online Banking Management
- Online Banking System - Account Opening
- Optical Imaging
- Peer Bank Analysis, Benchmarking and Credit Research
- Physical Security - Access Control
- Processing Services - Job Scheduling
- Program Management
- Project Management
- Purchase Ordering
- Real Estate Geographic Information System
- Real Estate Market Data and Analysis
- Real Estate Market Data and Sales Comparables
- Reg E Dispute Processing and Repository

- Regulatory Document Transmission
- Regulatory Reporting
- Remote Capture
- Resource Management
- Risk Management
- Rules-based Risk Rating, Suspicious Activity Monitoring and Reporting
- Secure File Transmission
- Securities Analysis
- Server Infrastructure
- Signature Card Image Capture
- Social Security Administration
- Tax Contract Management
- Technology - Active Directory Reporting
- Technology Asset Management
- Technology Management
- Technology Reporting
- Technology Utilities
- Telephony
- Teller Processing
- Third Party Return Check Reconciliation, Chargebacks
- Unclaimed Property Processing
- User Access Management
- Vendor Management
- Vendor Management - Monitoring
- Website Management
- Wire Transfer

12. Used For

A few words to describe the primary general function of the application service in its entirety. For example, “storage”, “processing”, “transmittal”, etc.

13. Technology Management Framework Identifier

Select the most appropriate purpose for the service using the *AFH TMF*. Developed in February 2020, the TMF provides a means to align assets of any type to the Bank’s core business objectives and other management purposes. The options are:

- **1A**: Grow Balance Sheet, Capital and Earnings
- **1B**: Cost Control, Flat Org Structure, Simple Product Line
- **1C**: Ongoing Enhancement of Governance Processes
- **1D**: Risk Reduction
- **1E**: Audit, Legal and Regulatory Compliance Remediation
- **2**: Maintenance & Day-to-Day Operations
- **3**: Enabling Business Improvement through Assessments and Upgrades
- **4**: Industry Framework Alignment

For example, the service Gmail by Google would most closely align to TMF category "2", *Maintenance & Support/Day-to-Day Operations*; while the Tenable Nessus vulnerability scanning service would fall into the category of "1D", *Risk Reduction*. Use your best judgement to determine.

14. **Owned By**
    The business line representative (employee name) responsible for the application service as applicable and the data contained within it. This individual and the Secondary Owner (below) are the only individuals authorized to approve access.

15. **Data Owner Department**
    The Owner's department as defined by Active Directory (pre-populated based on Owned By field).

16. **Functional Department**
    The Owner's functional department. This may be the same or different than the Data Owner Department.

17. **Secondary Owner**
    The business line representative (employee name or names) responsible as a backup or delegate for the application service as applicable and the data contained within it.

18. **Data Custodian**
    The person(s) responsible for the day-to-day activities related to access management for a particular application service.

19. **Data Steward**
    The individual(s) appointed by functional area senior leadership who act as the hands-on resource within the business to create / manage critical data elements, report data quality issues, and to conduct other data governance responsibilities around control and use of data. See the *AFH Data Governance Policy* for details.

20. **System User Department**
    The department identified as the primary user of the service. For example, "Audit Department", "Technology Department", "Information Security", or "The Whole Bank". Note this may be a different department than the *Data Owner Department* field.

21. **Interface to Core**
    Answer the question, "Does the service interface to the Core?" with yes or no.

22. **Interface to Other Applications**
    Answer the question, "What other key services [besides the Core] does the system interface with?" Enter the names of those services.

23. **IT Operating Model Identifier**
    The *IT Operating Model Standards* provides a means to clarify responsibilities for a given application service. The current selections are:

- **A1**: Applications Customized and Supported by Apple Bank. Hosted internally (Bank Data Center).
- **A2**: Applications Customized and Supported by Apple Bank. Hosted by a Cloud Infrastructure-as-a-Service (IaaS) provider.
- **B1**: Applications Customized and Supported by the Vendor. Hosted internally (Bank Data Center).
- **B2**: Applications Customized and Supported by the Vendor. Hosted by a Cloud IaaS or Platform-as-a-Service (PaaS) provider.
- **B3**: Applications Customized and Supported by the Vendor. Hosted by an Application Service Provider (ASP), or a Cloud Software-as-a-Service (SaaS) provider.
- **G1**: Bank-developed Applications. Hosted internally (Bank Data Center).
- **G2**: Bank-developed Applications. Hosted by a Cloud IaaS provider.

Additional details below:

<table>
<tr><th></th><th>A1</th><th>A2</th><th>B1</th><th>B2</th><th>B3</th><th>G1</th><th>G2</th></tr>
<tr><td>Description</td><td colspan="2">Appl. Customized and Supported by Bank</td><td colspan="3">Applications Customized and Supported by the Vendor</td><td colspan="2">Bank-developed Applications</td></tr>
<tr><td>Hosting Model</td><td>Internal Data Center</td><td>External (Cloud IaaS)</td><td>Internal Data Center</td><td>External (IaaS, PaaS)</td><td>External (ASP, SaaS)</td><td>Internal Data Center</td><td>External (Cloud IaaS) Future</td></tr>
<tr><td>Data Custodian</td><td colspan="7">Bank</td></tr>
<tr><td>App Uptime (SLA), DR Testing</td><td>Bank</td><td>Bank & Provider</td><td>Bank</td><td>Bank & Provider</td><td>Hosting Provider</td><td>Bank</td><td>Bank & Provider</td></tr>
<tr><td>Application Programming, Development</td><td colspan="5">Developer</td><td colspan="2">Bank</td></tr>
<tr><td>Application Security</td><td colspan="2" rowspan="2">Bank</td><td colspan="3">Application Developer & Provider</td><td colspan="2" rowspan="2">Bank</td></tr>
<tr><td>Change Mgmt., Maintenance Updates/Patches, End-user Support</td><td colspan="3">Application Vendor</td></tr>
<tr><td>User Access Administration</td><td colspan="7">Bank</td></tr>
<tr><td>Data Interfaces to Other Systems</td><td colspan="3">Bank</td><td>Bank or Provider</td><td>Hosting Provider</td><td colspan="2">Bank</td></tr>
<tr><td>Examples</td><td>FIS Miser, MISER-BI (EDW 1.0)</td><td>Future: Disaster Recovery (Virtual networking, storage)</td><td>BAM+, WirePro; and vendors Abrigo, Centurion</td><td>RingCentral, ServiceNow, Cisco VoIP, and future: VMware VCDR for DR Guest Apps</td><td>FIS IBS, FIS ImageCenter, Q2, McCracken, Remote Lender, Verafin, DMI Mortgage, Axiom; and Google Workspace; and future: IBM Blueworks, FOS</td><td colspan="2">EDW 2.0 (future), AppleNet Intranet, Report Development, IT Scripting</td></tr>
</table>

<table>
<tr><th></th><th>A1</th><th>A2</th><th>B1</th><th>B2</th><th>B3</th><th>G1</th><th>G2</th></tr>
<tr><td>Description</td><td colspan="2">Appl. Customized and Supported by Bank</td><td colspan="3">Applications Customized and Supported by the Vendor</td><td colspan="2">Bank-developed Applications</td></tr>
<tr><td>Hosting Model</td><td>Internal Data Center</td><td>External (Cloud IaaS)</td><td>Internal Data Center</td><td>External (IaaS, PaaS)</td><td>External (ASP, SaaS)</td><td>Internal Data Center</td><td>External (Cloud IaaS) Future</td></tr>
<tr><td>Data Custodian</td><td colspan="7">Bank</td></tr>
<tr><td>Environmental Controls, Physical Infrastructure & Uptime, Physical Security</td><td>Bank</td><td>Hosting Provider</td><td rowspan="2">Bank</td><td colspan="2">Hosting Provider</td><td>Bank</td><td>Hosting Provider</td></tr>
<tr><td>Logical Security, Logical Server Mgmt., OS Patching, Logical Network, Job Scheduling /Batch Processing</td><td colspan="2" rowspan="3">Bank</td><td>Bank or Provider (Depends on Application)</td><td>Hosting Provider</td><td colspan="2" rowspan="4">Bank</td></tr>
<tr><td>Operational Support</td><td colspan="3">Bank and Vendor</td></tr>
<tr><td>Backup</td><td rowspan="3">Bank</td><td colspan="2">Hosting Provider</td></tr>
<tr><td>Business Continuity Planning & DR Provisioning</td><td>Bank</td><td>Bank and Hosting Provider</td><td colspan="2">Bank and Hosting Provider</td></tr>
<tr><td>Asset Management</td><td colspan="3"></td><td>Bank</td><td>Bank and Provider</td></tr>
<tr><td>Examples</td><td>FIS Miser, MISER-BI (EDW 1.0)</td><td>Future: Disaster Recovery (Virtual networking, storage)</td><td>BAM+, WirePro; and vendors Abrigo, Centurion</td><td>RingCentral, ServiceNow, Cisco VoIP, and future: VMware VCDR for DR Guest Apps</td><td>FIS IBS, FIS ImageCenter, Q2, McCracken, Remote Lender, Verafin, DMI Mortgage, Axiom; and Google Workspace; and future: IBM Blueworks, FOS</td><td colspan="2">EDW 2.0 (future), AppleNet Intranet, Report Development, IT Scripting</td></tr>
</table>

24. <u>Internet Access</u>

Used to denote whether the application service is accessible via the Internet via a browser [only] or not. The field would not include those services which require an internally hosted system or service. Valid values are “Yes” and “No”.

25. <u>Administration Performed By</u>

This generally describes user administration (adding, setting permissions, etc.) Select from the following:

- **ABS**: For applications administered by the Bank.
- **Vendor**: For applications administered by the vendor or other 3rd party.
- **Hybrid**: For applications with management performed by both the Bank and vendor.

26. <u>Residing Location</u>

Answer the question, “Where does the service reside?” Use the server name if known (e.g., server name “ABS1NYC”) or use external hosting location (e.g., “Cloud” or “ASP”).

27. <u>Date Added</u>

Date the service was added. Be specific (e.g., “9/18/2020” versus “2020”).

28. <u>Comprising/Associated System/Investment</u>

Answer the question, “What system or other investment comprises this application or software?” For example, the software may be one tool of several used for “Vulnerability Management”. Note this is different and more detailed than the overarching Business Function of “Information Security”.

29. **License Required**
    Answer the question, “Is a license required for use?” with yes or no.

30. **Number of Licenses Purchased**
    If a license is required, answer the question, “How many licenses have been purchased?” with a number. If no license is required, answer “N/A”.

31. **Number of Licenses Deployed/Used**
    If licenses have been purchased, answer the question, “How many licenses have been deployed or used?” with a number. If no license is required, answer “N/A”.

32. **Bank’s End of Useful Life (EoUL) Date**
    The point in time in which an application service has/will fulfill the purpose for which it was required. This point-in-time may or may not match the End-of-Life cycle indicated by the vendor or manufacturer. Reasons for invoking EoUL may include but are not limited to newer technology, degraded performance, incompatibility or security concerns. Enter the date and be as specific as possible. If this date is in the past, use the past date.

33. **Vendor’s End of Life (EoL)**
    The point in time when the support vendor indicates that an application service has reached the end of its useful life. At this point, the vendor will either end or limit support for the service. Extended support [including bug-fixes and security updates] may be available after this point, typically for a fee. Enter the date and be as specific as possible. If this date is in the past, use the past date. If you do not know, please confirm with the vendor.

34. **Vendor’s End of Support (EoS)**
    The point in time when the support vendor indicates that it will no longer provide extended support [including bug-fixes and/or security updates] for an application service, even for a fee. This might not be the same as the vendor’s EoL date, for example, if an extended maintenance support contract is in place and the vendor is providing security patches/bug fixes. Enter the date and be as specific as possible. If this date is in the past, use the past date and seek management support to discuss the issue. If you do not know, please confirm with the vendor.

35. **Maintenance Contract Status**
    Answer the question, “Is the application service within the maintenance contract/support period?” with “Yes” or “No”. If no or if the support has ended, seek management support to discuss the issue.

36. **Data Classification**
    This relates to the data stored, processed, transmitted or received by the application service. Select one of the following, as outlined in the *AFH Data Classification Policy*:

- **Confidential**: The highest level of data classification. Unauthorized disclosure, compromise, or destruction of this information could provide a significant advantage to a competitor, or result in severe damage and penalties to the Bank, its clients, customers, business relations, counterparties or employees. It is intended solely for use within the Bank. Access is limited to those with an explicit, predetermined and stringent "business need-to-know", and is further limited to the lowest level of access necessary to fulfill the business requirements.

  Examples: Customer sensitive information (personally-identifiable information [PII], customer non-public information [NPI], board information, proprietary bank information, employee health records, audit reports, encryption keys and passwords, security logs, etc.
- **Restricted**: The second highest data classification, and is information that is designated by the Data Steward (or otherwise) as Restricted. Unauthorized disclosure, compromise, or destruction of this information could - directly or indirectly - result in significant adverse impact on the Bank, its clients, customers, business relations, counterparties, vendors, third-party service providers or employees. Adverse impacts may include financial loss, damage to reputation, loss of business, jeopardy to the security of organizational assets, and potential legal action. Restricted information is intended primarily for use within the organization and access is limited to those with "business need-to-know" and non-Bank personnel covered by a non-disclosure agreement.

  Examples: System configurations, personnel records, budget information, security plans/standards, network diagrams, marketing and sales plans, business email addresses, purchase orders, bank policies/procedures/processes, vendor and supplier lists, etc.
- **Internal**: Primarily internal or proprietary information not meant for public knowledge or disclosure. Unauthorized disclosure, compromise, or destruction may result in some adverse impact to the organization, its customers, or employees. Due to its technical or business sensitivity, access is limited to employees and non-Bank personnel subject to a non-disclosure agreement.

  Examples: Telephone directory, organization charts, routine administrative/office information, employee status and work history, bank advertising details.
- **Public**: Information that can be disclosed to anyone or has been previously released into the public domain. Unauthorized disclosure, compromise, or destruction would neither violate an individual's expectation of privacy, expose the organization to financial loss or embarrassment, nor jeopardize the security of company assets. Although Public Information generally may be disclosed, disclosure of Public Information must not violate any pre-existing, signed non-disclosure agreements (see Confidential, above).

  Examples: Marketing brochures, published annual reports, interviews with news media, business cards, public press releases, public portions of the organization's web sites, publicly-posted job announcements.

See the *Data Classification Policy* for additional guidance and examples.

37. <u>Financial Exposure</u>

The dollar amount of transactions processed by the application service for a given period of time (preferably one year) which indicates the importance to the primary users (data owner) of the service. Select:

< $1 Million
$1 Million - $10 Million
$10 Million - $50 Million
> $50 Million
N/A if None

38. Data Retention Schedule

Answer the question, "How long is the data required to be retained for compliance purposes or Bank requirements?" For example, "5 years". Refer to the *Record Retention and Disposal Policy* and *Record Retention Schedule* for details.

39. Recovery Time Objective

Answer the question, "How soon after a disaster does the service need to be restored?" Select from the following:

Immediate
<=4 hrs
<=8 hrs
<=12 hrs
<=24 hrs
<=48 hrs
<=72 hrs
<=96 hrs
<=120 hrs
<=1 week
<=2 weeks
<=3 weeks
<=4 weeks
<=8 weeks
<=12 weeks
> 12 weeks

If the answer is unknown, seek input from the Business Impact Analysis and Disaster Recovery Plan for the specific application, or guidance from the BCP/DR team within the Technology IT GRC-CM department.

40. Most Recent Contingency Test

Enter the date of the most recent contingency test (e.g., "12/19/2019"). Leave blank if the service is not required to be tested per the BCP Plan. Seek guidance from the BCP/DR team within the Technology IT GRC-CM department.

41. Financial/Regulatory Reporting Indicator

Answer "Yes" for services which are considered a support system used for financial or regulatory reporting. Answer "No" for all others.

42. **Inherent Risk Score**

    Data captured during the most recent Information Security Application Risk Assessment. Answer should be IR-01 through IR-08 or "Assessment Not Performed". If the assessment is not required to be completed, answer "N/A". Seek guidance from the Information Security department.

43. **Security Risk**

    Answer as follows:

    - **High**: Compromise of this service or the information stored/processed/transmitted/received by the service could result in extreme damage to the organization and/or its customers.
    - **Medium**: Compromise of this service or the information stored/processed/transmitted/received by the service could result in temporary disruptions or loss of customer confidence and trust.
    - **Low**: Compromise of this service or the information stored/processed/transmitted/received by the service could result in minor inconvenience and temporary loss of productivity.
    - **N/A**: Not applicable, for example, if the service does not store, process, transmit/receive information. This answer should rarely be used.

44. **Password Policy Compliance**

    Answer the question, "Does the service's authentication mechanism allow compliance with the Bank's password policy?" "Yes" or "No".

45. **Active Directory Integrated**

    Answer the question, "Is the service's authentication mechanism integrated into the Bank's Active Directory system?" (i.e., single sign-on). "Yes" or "No". Answer "N/A" if not applicable.

46. **MFA**

    Answer the question, "Is the service's authentication mechanism utilizing multi-factor authentication (MFA; e.g., a username/password and soft token/code)?" "Yes" or "No". Answer "N/A" if not applicable.

47. **Requires Data Governance**

    An indicator to identify if the application service falls under the scope of the Data Governance program. Data Governance Program scope includes establishing a Data Dictionary of Key Business Terms and Definitions, documenting end-to-end data flows, and creating data quality rules to perform ongoing tests of data quality for critical data elements. Valid values are "Yes", "No" or blank. Seek guidance from the Data Governance team as needed.

48. **Business Data Domain**

    [Used only if "Requires Data Governance" is "Yes".] Data Domains are the primary vehicle for assigning data management accountability. A Data Domain is a logical grouping of data, based on shared characteristics (e.g., retail banking data, customer and account data, etc.) Seek guidance from the Data Governance team as needed.

49. **System of Record, System of Origin Indicator**

    [Used only if "Requires Data Governance" is "Yes".] A SOO is an information system that generates or creates physical data elements. A SOR is the authoritative system accountable for active data

management, operational maintenance, and validation of a specific set of physical data elements. A system can have both SOO and SOR components. Valid values for this field are SOO, SOR, SOO and SOR, or leave blank. Seek guidance from the Data Governance team as needed.

50. SOO/SOR Information

[Used only if "Requires Data Governance" is "Yes".] Used in conjunction with the SOO/SOR indicator and details the business application SOO/SOR information being made available for use in the Bank's critical business reports and processes. Seek guidance from the Data Governance team as needed.

51. Personal Data

Flag indicator to identify if the application service contains any information that is linked or reasonably linkable to an identified or identifiable person. Personal Data is characterized as *Confidential Data* or *Restricted Data*, depending on the level of sensitivity. Valid values are "Yes", "No" or "N/A". This is a Data Governance-related field.