Vendor Risk Management

Turn on audio 

Apple Bank

What is Vendor Risk Management?

- A Vendor is a third-party with which the Bank has entered into a formal, contractual business relationship for the purposes of supporting the Bank by providing outsourced services and/or products that the Bank needs to operate or desires to offer to customers

- Vendor Risk Management (VRM) is the process of identifying all significant vendors that aid in the delivery of products and services to the Bank and/or to our customers on behalf of the Bank, while assessing, managing, and taking steps to mitigate the risks potentially associated with those vendors

- The VRM team collaborates with internal stakeholders such as Data Privacy, Legal, Information Security, and Business Owner throughout the vendor risk management process

- The VRM team provides oversight and accountability over vendor relationships, provides independent review and assessment of vendors and maintains the documentation and reporting on vendors

Why is Vendor Risk Management Important?

Vendor risk management is not only a regulatory requirement, but also a strategic advantage

Regulatory

- Enforcement actions are increasing
- We could be fined (which can get costly)
- Getting in trouble with a regulator can lead to bad press and hurt reputation

Strategic

- It protects our organization
- Improves our organization's cybersecurity profile
- Have more knowledge on a vendor before signing the contract
- Cost savings in contract terms, missed renewals & improved service
- Ensure our vendors are performing as agreed
- Reduce the potential for disruption to operations

Regulatory Guidance

There is a heightened focus on vendor risk by multiple regulators

OCC Bulletin 1999-14

FIL-49-1999
Bank Service Company Act

FIL-50-2001
Bank Technology Bulletin: Technology Outsourcing Information Documents

FIL-68-2001
501(b) Examination Guidance

FIL-23-2002
Country Risk Management

FIL-121-2004
Computer Software Due Diligence

FIL-27-2005
Guidance on Response Programs

FIL-81-2000
Risk Management of Technology Outsourcing

FIL-22-2001
Security Standards for Customer Information

Outsourcing Technology Services

FDIC FIL-104-2005

FIL-52-2006
Foreign-Based Third-Party Service Providers

FIL-105-2007
Revised IT Officer's Questionnaire

NCUA 08-cu-09
Evaluating Third-Party Relationships Questionnaire

NCUA 2007-cu-13
Evaluating Third-Party Relationships

FIL-44-2008
Guidance for Managing Third-Party Risk

FIL-127-2008
Guidance for Payment Processor Relationships

OCC Bulletin 2010-30

FINRA Rule 3190

FINRA Regulatory Notice 11-14

FFIEC OT Exam Handbook Supervision of Technology Service Providers

FIL-3-2012
Managing Third-Party Payment Processor Risk

CFPB 2012-03
Service Providers

OCC-2013-29
Guidance on Third-Party Relationships

Federal Reserve SR 13-19/CA 13-21
Guidance on Managing Outsourcing Risk

FFIEC Social Media Guidance

FFIEC IT Examination Handbook

OCC-2017-7
Supplemental Examination Procedures for Risk Management of Third-Party Relationships

OCC-2020-10
Frequently Asked Questions to Supplement OCC Bulletin 2013-29

NCUA SL-17-01
Evaluating Compliance Risk

OCC-2017-43
Risk Management Principles

FIL-19-2019
Technology Service Provider Contracts

OCC Bulletin 2019-43

OCC Bulletin 2019-45

OCC-2020-65
UDAP/UDAAP Exam Procedures

Vendor Risks

Primary risks VRM focusses on:

- **Operational Risk**: Operational risk is the risk that a vendor's operations or systems will not perform properly and result in losses due to: inadequate or failed internal processes, employee error, system failures, etc.
- **Regulatory Risk:** Regulatory risk arises when a vendor's operations are not consistent with laws, regulations, ethical standards, or the bank's policies and procedures
- **Reputational Risk:** Reputational risk is risk of vendors having a negative impact on Apple Bank's reputation due to but not limited to negative publicity, regulatory violations, data breaches, etc. As risk of data loss and risk of service failure increase, the bank's reputational risk also increases
- **Concentration Risk**: Concentration risk is risk of Apple Bank heavily depending on a particular vendor for multiple activities, particularly when several of the activities are critical to bank operations

Business Owner and Vendor Risk Management Responsibilities

Business Owner

- Contact VRM of any new or revised relationship with vendor
- Complete an intake form for each vendor or vendor relationship being on boarded
- Monitor vendor performance and alert VRM of any issues
- Inform Legal and VRM of proposed additional contractual agreements with vendor
- Notify VRM of vendor merger and / or name change
- Consult with Legal prior to, and advise VRM after vendor termination
- In the event of a data security incident, Business Owners must notify VRM, InfoSec, Privacy, and Legal

You own the Risk!

VRM

- Track and maintain due diligence document inventory
- Obtain updated documentation from vendor
- Perform vendor reviews for tiers 1, 2, 3 confirming vendor controls and performance
- Conduct annual confirmation of vendor relationships with Business Owners

Vendor Risk Management Process

Structured and disciplined process across the life of an engagement

Onboarding

Intake form, control surveys, documentation collection and risk scoring

Vendor Intake and Risk Assessment

Understand the risk the engagement could pose and how critical the vendor is (or will be) to Apple Bank

Contract Review and Approval

After Legal review and approval to obtain robust and sound written agreements with vendors, VRM confirms proper execution and signing authority and archives appropriate contract documentation

Ongoing Monitoring

Monitor vendors' performance and well-being throughout the engagement and conduct periodic assessments to:

1) verify vendors still meet expectations,
2) identify areas of concern, and
3) discover contract gaps, poor vendor trends and declining service levels

Off-boarding

Verify with Legal consultation, as appropriate, that contract exit requirements are met

Vendor Onboarding Steps

What to Consider When Onboarding a Vendor

Onboarding

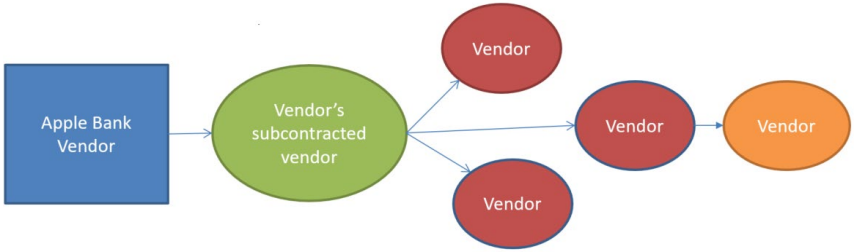
Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

- ✓ Will the vendor have access to data? If so, what type of data?
- ✓ Will the vendor store, process, or transmit the data?
- ✓ Will the vendor have access, host or transmit to the Bank's network?
- ✓ Will the vendor outsource or subcontract to their vendors who will have access to our data and who are they?



- ✓ How critical is the service that this vendor is providing?
- ✓ How long have they been in business?
- ✓ What is their financial condition?
- ✓ Do the services fall under the Bank Service Company Act (BSCA)?

  check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, other clerical, bookkeeping, accounting, statistical, or similar functions such as data processing, Internet banking, or mobile banking services

Vendor Onboarding Steps

Structured and disciplined process; all vendors entered into risk system; all vendors risk reviewed

Onboarding

- Business Owners fill out a Vendor Intake Form that contains weighted questions
- Vendor is accepted into VRM Risk Management System (“RaaS”) as a ‘pending’ vendor
- VRM reviews the Vendor Intake form, risk level assigned one of five tiers {1, 2, 3, 4, 5}

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

Vendor Onboarding Steps

Monitoring multiple Relationships and different Business Owners with the same vendor

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

- VRM tracks and monitors multiple relationships with a single vendor
- When engaging services with a vendor, log into RaaS to see if the vendor already exists
- If the vendor exists already in RaaS, you may add an additional relationship to the vendor
- If you do not have access to the vendor, contact VRM
- Be sure to give a complete description of the service the vendor will provide in the description field within the Intake Form

Risk Tiers

Clear requirements based on risk; per SR 13-19, oversight commensurate with the risk presented

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

VM - Scoring Tier Matrix			
Tier	**Score**	**Description**	**Requirements**
Tier 1	[80+]	Critical risk vendor. These vendors represent a significant risk to business practices, have access to confidential or restrictive such as Customer information, data protected by the Gramm-Leach-Bliley Act (GLBA), network access, PCI, off-sight data storage, vendor criticality, significant penalties and restitution if vendor is not compliant. These vendors need to be continually monitored for regulatory compliance and to ensure adequate risk controls are in place.	- Annual survey - Quarterly financial health monitoring - Due diligence documentation - Monthly Regulatory monitoring - Real time negative news monitoring
Tier 2	[60-79]	High risk vendor, have access to confidential or restrictive such as customer information data protected by the Gramm-Leach-Bliley Act (GLBA), Employee information, physical retention of off-sight storage, vendor criticality, confidential supervisory information, moderate risk of legal or regulation non-compliance with the type of service offered by vendor. These vendors needs to be continually monitored for regulatory compliance and to ensure adequate risk controls are in place.	- Annual survey - Quarterly financial health monitoring - Due diligence documentation - Monthly regulatory monitoring - Real time negative news monitoring
Tier 3	[40-59]	Medium risk vendor with access to Bank Confidential/proprietary information such as: financial statements, performance and reporting data, Board & Committee information, Audit reports, etc.	- Biennial survey - Quarterly financial health monitoring - Due diligence documentation - Monthly regulatory monitoring - Real time negative news monitoring
Tier 4	[20-39]	Low risk vendors that represent limited risk to the organization, do not touch sensitive data, and vendor failure will not have a material impact on your institution.	- Annual financial check at initial review - Annual Regulatory check at initial review
Tier 5	[0-19]	Limited to no risk to the institution.	- Annual financial check at initial review - Annual regulatory check at initial review

Apple Bank

Vendor Intake and Risk Assessment

Additional information collected based on risk and nature of the specific engagement

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

- Tier 1, 2, 3 vendors are issued a Vendor Control Survey
- Vendor completes the Control Survey and upload requested due diligence documentation
- Control survey and due diligence documentation reviewed by VRM and InfoSec
- After InfoSec approval, Business Owner receives an email to approve the vendor profile

Contract Review and Approval

VRM works closely with Legal Department; gated Contract Execution Approval to ensure process is complete

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

- Draft contract forwarded to Legal Department; Bank's attorney makes necessary contract edits that are agreeable to vendor and Business Owner
- After Legal has reviewed the contract, Bank's attorney will sign the Contract Execution Approval form and send it along with the contract to Privacy, InfoSec and VRM to sign, copying the Business Owner
- VRM signs Contract Execution Approval form last to ensure process is complete and alerts Business Owner
- Contract can now be signed by the Business Owner and the Vendor
- Business Owner sends fully executed contract to VRM to be filed in RaaS
- The vendor status in RaaS changed to 'approved vendor'

Apple Bank Vendors

VRM overseeing vendor relationships; oversight commensurate with the risk presented

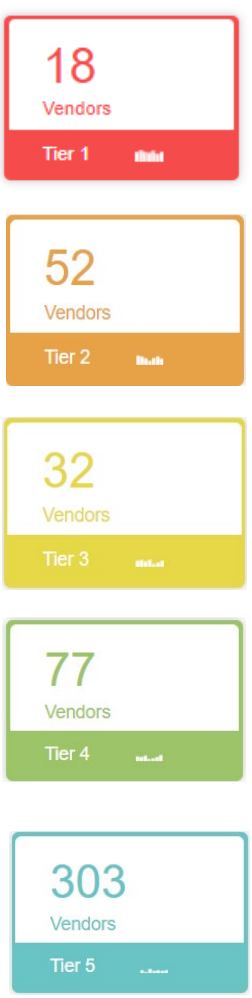
Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding



Critical risk vendor: These vendors represent a significant inherent risk to business practices, have access to confidential or restricted data such as Customer information, data governed by the Gramm-Leach-Bliley Act (GLBA), network access, PCI, compliance obligations, off-sight data storage, vendor criticality, present risk of significant penalties and restitution if vendor is not compliant; these vendors are continually monitored for regulatory compliance and to ensure adequate risk controls are in place

High risk vendor: These vendors present risks arising from having access to confidential or restricted data such as customer data governed by the GLBA, employee information, and physical retention of off-sight storage, vendor criticality, confidential supervisory information, moderate risk of legal or regulation non-compliance with the type of service offered by vendor; these vendors' are continually monitored for regulatory compliance and to ensure adequate risk controls are in place

Medium risk vendor: These vendors have access to Bank Confidential/proprietary information such as: financial statements, performance and reporting data, Board & Committee information, Audit reports, etc.

Low risk vendors: These vendors present limited risk to the organization, do not touch sensitive data, and vendor failure will not have a material impact on Apple Bank.

(*really*) **Low Risk vendors:** Limited risk to the institution (examples: advertising agencies, postage, office supplies, etc.)

Ongoing Monitoring Activities

Ongoing monitoring is an active partnership between VRM and Business Owners

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

Business Owner

- Monitor vendor performance and alert VRM of any issues
- Contact VRM regarding any new or revised relationship with vendor
- Inform Legal and VRM of additional contractual agreements with vendor
- Notify VRM of vendor merger and / or name change
- Advise VRM of intended vendor termination

VRM

- Track and maintain due diligence document inventory
- Update expired documentation
- Confirming vendor controls (i.e. Soc-2) and service performance
- Annual confirmation of the nature of vendor relationships with Business Owners
- Reconciliation with Accounts Payable for invoices and corporate credit cards

Off-boarding a Vendor

When services are ending, take stock as to what Bank information your vendor has

Onboarding

Vendor Intake and Risk Assessment

Contract Review and Approval

Ongoing Monitoring

Off-boarding

- Has the vendor completed the engagement successfully?
- Has the vendor returned or destroyed confidential data and appropriately certified to such?
- Notify Vendor Risk Management when the engagement is naturally ending or is being terminated to inactivate the vendor in the system
- Seek legal counsel if you are considering terminating the contract!

Key Contacts

- Vendor Risk Management: Vendormgmt@applebank.com
- Contract Review: Vendorcontractapprovals@applebank.com
- Information Security: Infosec@applebank.com
- Privacy: Privacy@applebank.com

You have completed the presentation.

Select "**Vendor Risk Management Attestation Test**" to complete the attestation and receive credit for completing the course.