Vendor Management w/Northrim

Overview of VM Program and

Due Diligence

Douglas Frey, SVP, Information Security Officer
Tze "Z" Teoh, AVP, Cybersecurity Program Manager

Northrim Bank®

Agenda

Background

Initial Vendor Due Diligence Process

- Assign Category
- Strat Plan
- Form Team and Review Demo
- Document Collection & Actual Due Diligence Methodology
- Conclusion and Report

Recurring Due Diligence (aka Management Review)

- Use of Venminder
- Repeat DD Steps based on Vendor Category

Who We Are

- Publicly Traded Community Bank (NRIM) based in Anchorage, Alaska
  - ~450 Employees, $2.6B Assets
  - 17 Branches Located throughout Alaska
  - 2 Loan Production Offices
  - 1 Asset Based Lending Division in Washington
  - Residential Mortgage LLC, wholly owned subsidiary
- Insured and regulated by FDIC, subject to SOX, Internal and External Audits
- Our VM and DD program works for us – Your Mileage May Vary!!

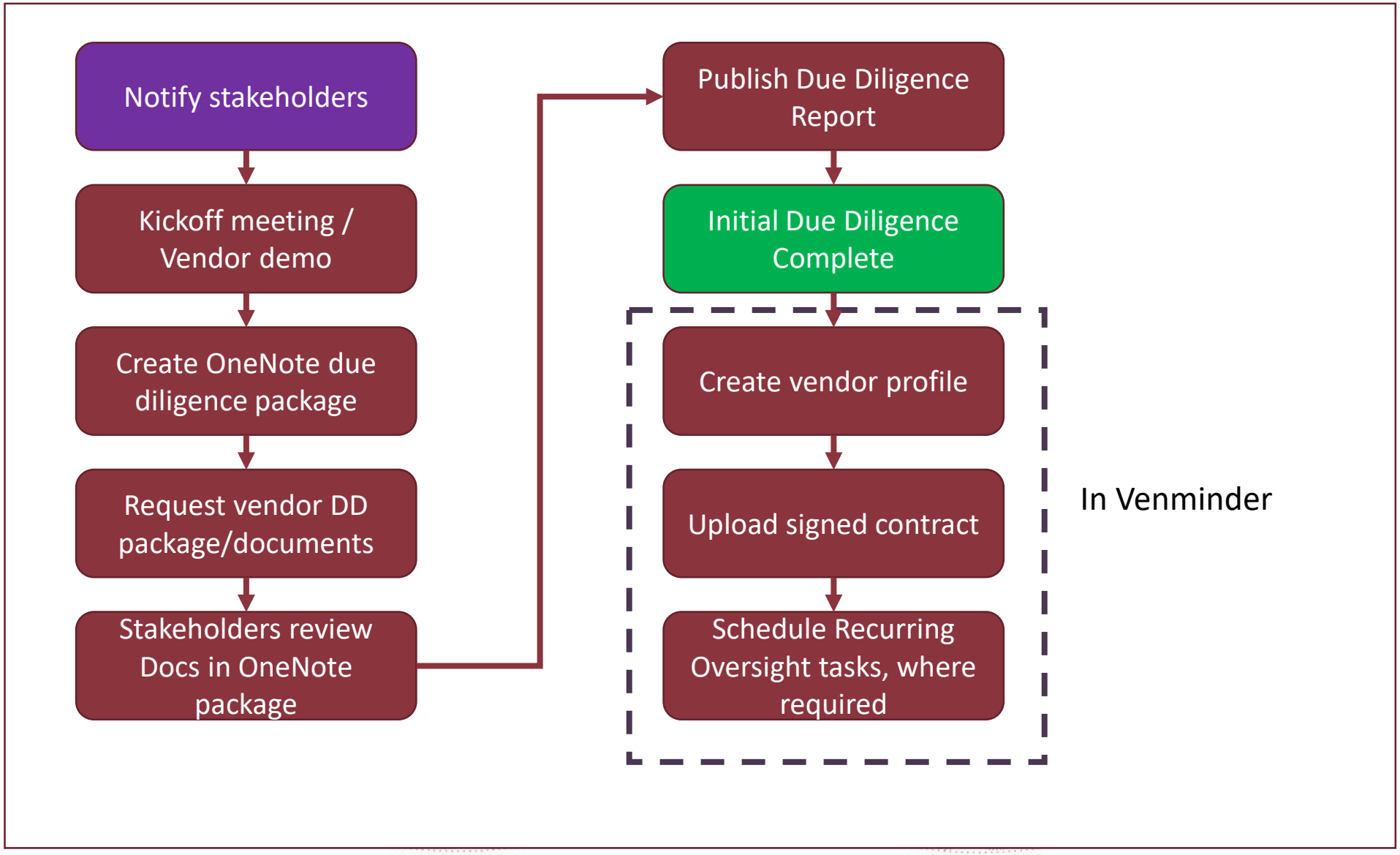
Assign Category

- All Vendors are divided into 2 groups:
  - Non-Technology Service Provider (aka Vendor)
    - Appraisers, attorneys, landscapers, window washers, janitors, etc.
    - Managed by spreadsheet and coordinated with Accounting
  - Technology Service Providers (aka TSP)
    - Core Provider, Loan Origination Software, Software as a Solution Providers
    - Managed in Venminder

Technology Service Providers

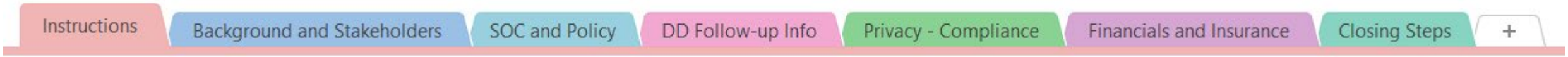
- All Technology Projects/Solutions must be sponsored by an Exec, Approved by CIO, and outlined in Board-Approved Strategic Plan
  - Sponsor works with CIO on timing and future year requirements which are codified in Strat Plan
- Sponsor shortlists potential TSPs
  - Organizes/Identifies Stakeholders & Schedules Demos
    - Stakeholders always include IT, InfoSec, Compliance, Risk, and Legal
      - May Include Marketing, Accounting, etc.
- Due Diligence Package Created

Due Diligence Process



Due Diligence Package

- Due Diligence Package Created – Documents Requested
  - We use Microsoft OneNote
  - The tabs in the OneNote are shown below:



- Documents request list includes:
  - SOC 2 Type 2 Report
  - TSP's Security Policies
  - Brief description on how non-public information (NPI) will be securely transmitted to or accessed by the potential TSP
  - Most recent annual Pen-Test results
  - Most recent annual Disaster Recovery results
  - Latest Certificate of Insurance, including Cyber liability

Due Diligence Package

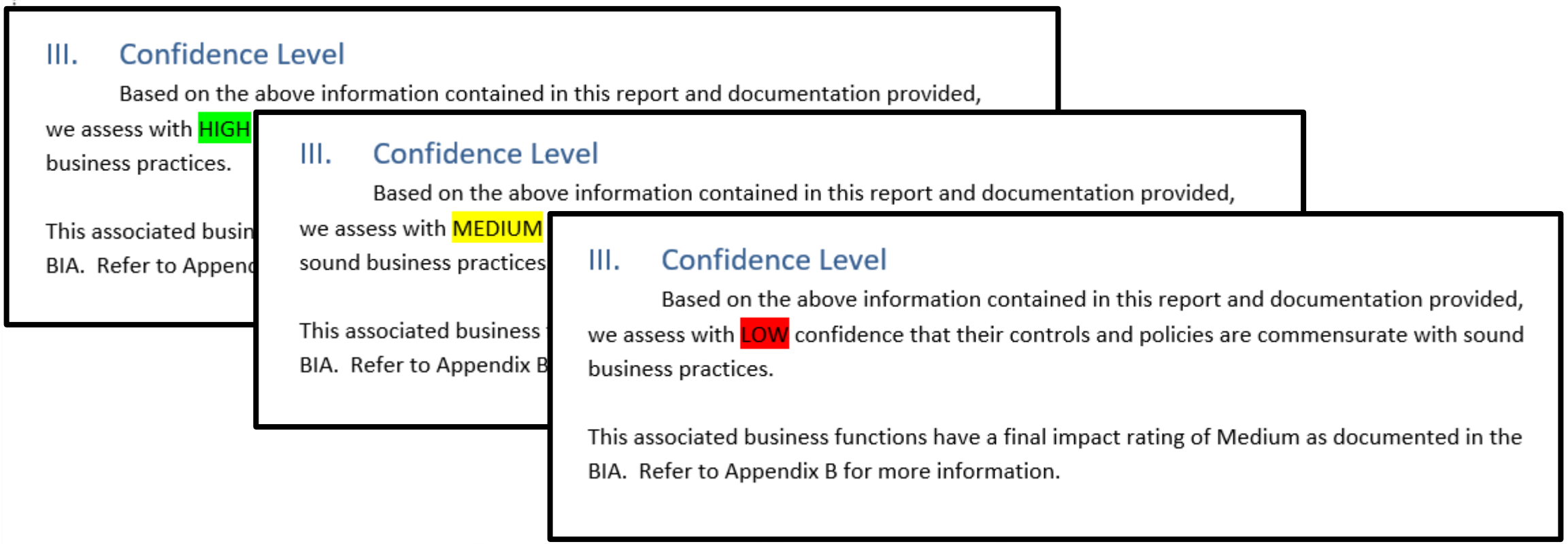
- We do not use Questionnaires unless TSP fails to provide adequate information in their existing Vendor DD Package
  - We appreciate TSPs who provides a completed Standardized Information Gathering (SIG) questionnaire which aides to clarify DD requirements
    - Venminder has SIG Questionnaire templates which can be used to solicit info from TSPs
    - Venminder Home > Questionnaire > Edit > Create Questionnaire > Load Template
- Once completed – A Final Report is issued and provided to the Sponsor & Relationship Owner
- Closeout tasks are documented

Due Diligence Report (Cont'd)

Contents

Due Diligence Report

- We are not decision makers – we are Subject Matter Experts



III. Confidence Level

Based on the above information contained in this report and documentation provided, we assess with HIGH business practices.

This associated busin
BIA. Refer to Appen

III. Confidence Level

Based on the above information contained in this report and documentation provided, we assess with MEDIUM sound business practices

This associated business
BIA. Refer to Appendix B

III. Confidence Level

Based on the above information contained in this report and documentation provided, we assess with LOW confidence that their controls and policies are commensurate with sound business practices.

This associated business functions have a final impact rating of Medium as documented in the BIA. Refer to Appendix B for more information.

Employing Venminder

- Upload Docs, Assign Relationship Owner, Enter Contract Expiration Date, Create recurring oversight tasks
- Assign Vendor Rating
  - Critical = Any TSP involved in the production or record keeping and used for Financial Reporting (also known as Sarbanes Oxley (SOX) Act of 2002)
  - High = Any non-SOX related TSP where access to NPI is provided; any TSP whose business function has been rated as High*
  - Low = Non-Critical

Secure Your Crown Jewels

- "He who defends everything, defends nothing" -- Frederick the Great
- Focus on your "top/critical" vendors
- Identify all TSPs that receive customer/NPI from your organization
- Ensure these TSPs have adequate controls in place, e.g.
  - ✓ Encryption in-transit, at-rest
  - ✓ Multi-factor authentication
  - ✓ Cyber liability Insurance coverage
  - ✓ Data destruction/deletion upon contract termination

Questions?

Northrim Bank®