A HIGH-LEVEL OVERVIEW TO VENDOR RISK MANAGEMENT

Vendor Risk Management Cheat Sheet

What Is Vendor Risk Management?

Most organizations rely on vendors to provide various products and services. Vendors can either support the organization itself and/or its customers. These vendor relationships can be necessary and valuable, but they also involve risk, which must be identified, assessed, managed, and monitored. This end-to-end process is often referred to as "vendor risk management," "vendor management," or the term "third-party risk management."

Governance Documentation

An effective vendor risk management program should be built on a foundation of formal governance documentation that defines the rules and requirements of the program. These documents generally include a policy, program, and set of procedures that guide your vendor risk management program to success.

Download our **How-To Guide: Developing and Maintaining Mature Third-Party Risk Management Governance Documentation eBook.**

DOWNLOAD NOW

1. **The policy is the organization's governing rules, boundaries, and guidelines for vendor risk management.** *It defines the regulatory guidelines or expected standards the vendor risk management program must meet. It identifies the program's scope, oversight and governance, roles and responsibilities, and how issues are managed.*
2. **The program document provides a detailed overview of the vendor risk management processes used to meet the policy's requirements.** *The program further defines objectives, requirements, roles, responsibilities, and deliverables for each lifecycle stage, from onboarding to offboarding. It details workflows, activity timing, and approvals.*
3. **Procedures are detailed step-by-step instructions on how to complete the vendor risk management processes.** *These are also called desktop procedures or user guides, and are used to provide information on daily tasks and activities.*

While all governance documents are important, you'll be asked to present your policy during an audit or regulatory exam. The policy should be reviewed and approved by the board (or senior management if there is no board) on an annual basis.

Your program document provides detailed information to senior management and stakeholders but may also be shared with auditors or examiners. It should be reviewed annually and updated when necessary.

Procedures help ensure all tasks and activities are completed on time and correctly. Procedures can be reviewed and updated as necessary.

Vendor Risk Management Lifecycle

The Foundation – Three Essential Elements of the Vendor Risk Management Lifecycle

OVERSIGHT & ACCOUNTABILITY

It's important to understand who will oversee third parties and who will be responsible for each task and function within the lifecycle. Consider how the vendor risk management program exists within the enterprise risk or compliance management framework.

DOCUMENTATION & REPORTING

Vendor risk management governance documents are used to assist in communicating the requirements, roles, and responsibilities of the overall program. Other documents, such as vendor risk reviews and control documents provide evidence of program compliance and must be maintained. Formal reporting requirements must be documented in policies and programs. Regular reporting ensures stakeholders are informed of relevant data to drive actions and decisions.

INDEPENDENT REVIEW

An internal or external review from independent auditors or third-party assessors helps ensure your program complies with regulatory requirements, best practices, or certification standards.

The 3 Stages of the Vendor Risk Management Lifecycle

1 ONBOARDING
Understanding the amount and types of vendor risk and validating vendor controls

PLANNING & RISK ASSESSMENT

Perform a risk assessment to determine the inherent risk and criticality of the vendor. Inherent risk is naturally present in the product and service of the relationship, and is assessed without consideration of any future controls. Criticality reflects the potential impact on the organization's operations should the vendor fail or go out of business.

DUE DILIGENCE

Do your homework before entering a business relationship with the vendor. Collect and review information about the vendor's risk management practices and controls. The level of due diligence varies, as it's dependent on the vendor relationship, but some examples of due diligence you may collect and review are business continuity (BC) and disaster recovery (DR) plans, audited financial statements, SOC reports, and more. This process will validate the effectiveness of mitigating controls and help you determine the engagement's residual (remaining) risk.

CONTRACTING

If you've determined the vendor risk is acceptable, you're ready to formally select the vendor and consider the contract. Ensure your contract is well-written to protect your organization and its customers against risk. When reviewing existing vendor relationships, use due diligence assessment information to determine whether any contract provisions need to be added or re-negotiated.

2 ONGOING
Staying aware of new or evolving risks

RE-ASSESSMENTS

Lines of business or vendor owners should confirm whether the vendor's risk has changed by reviewing and updating the inherent risk assessment on a predetermined schedule. Critical and high-risk vendors should be re-assessed at least annually. Moderate-risk vendors can be assessed every 18 months to two years, and low-risk vendors every two to three years or before contract renewal.

DUE DILIGENCE

Collecting and reviewing vendor due diligence should be done throughout the engagement, not just at the beginning. A vendor's risk and controls can change, so scheduling a due diligence review at least annually is best. This review should occur in tandem with the risk re-assessment. Reviews should also be done before contract renewals or in the case of performance issues and new or updated regulations. Even if there are no new or emerging risks, collect updated due diligence documents and replace expired SOC reports or insurance certificates, for example.

MONITORING & PERFORMANCE

Re-assessments are a critical activity, but it's also important to continually monitor the vendor's risk and performance to ensure consistency. Keeping track of your service level agreement (SLA) and staying informed of any issues or changes can help you determine if the cost/risk-to-benefit ratio has changed enough to terminate the relationship.

RENEWALS

Contract renewals should be planned well in advance, so you have enough time to negotiate any changes if needed. You should maintain a continuous dialogue with your vendor about service delivery, performance, and any service level gaps as part of ongoing contract management.

3 OFFBOARDING
Ending the vendor engagement

TERMINATION

When it's time for the vendor engagement to end, you'll need to notify the vendor that the contract won't be renewed. However, the vendor will still be in the lifecycle for the duration of the contract.

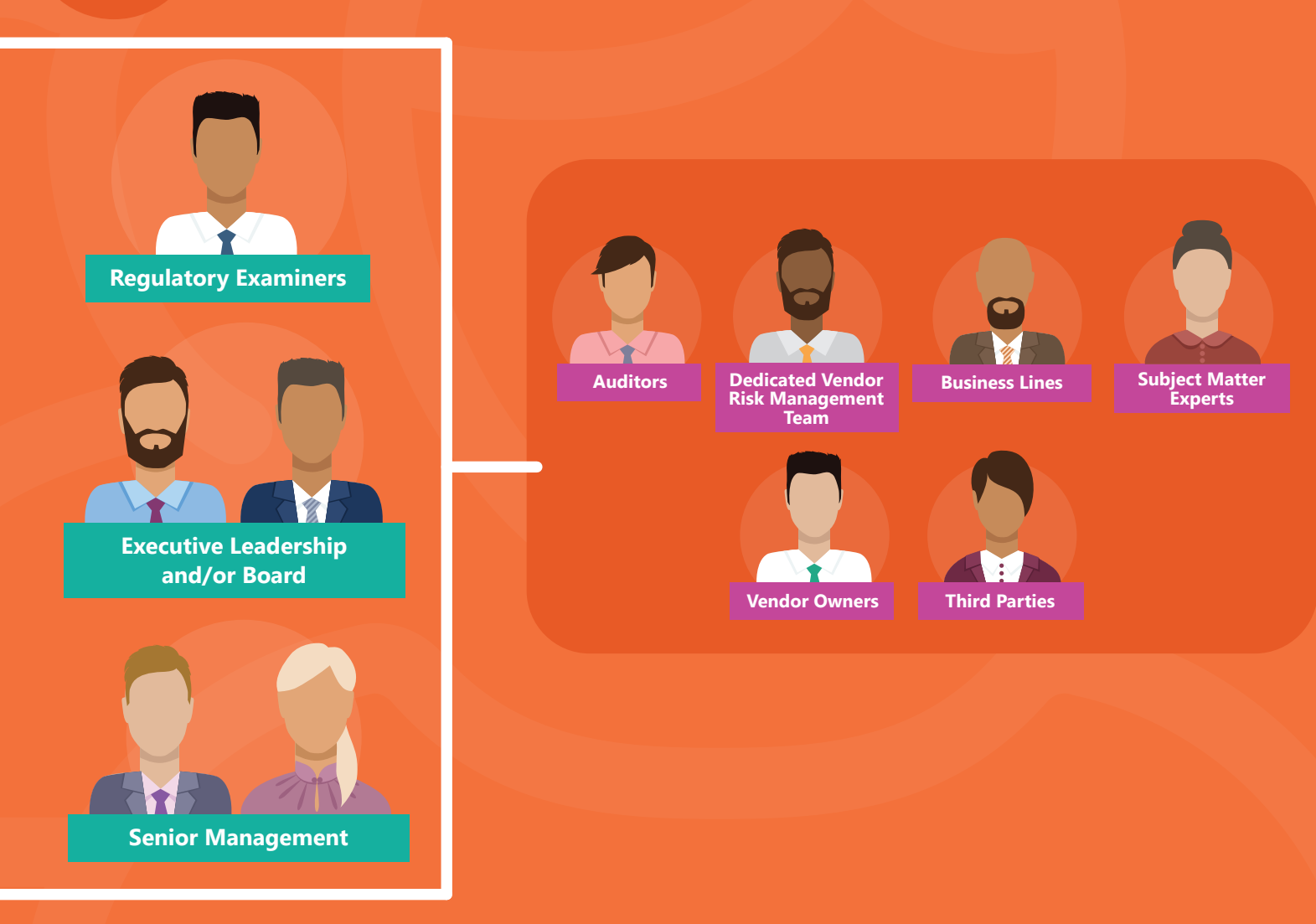
EXIT PLAN EXECUTION

Whether you bring the activity in-house or transition to a new vendor, an exit plan outlining both parties' responsibilities should already be established. Your vendor may be responsible for returning or destroying sensitive data. At the same time, your organization needs to revoke the vendor's access to your systems and facilities.

TPRM CLOSURE

You may still need to complete a few final steps to formally close the vendor relationship, such as paying final invoices and filing or archiving relevant vendor information.

Who Is Involved?



Download our **Framework for a Successful Third-Party Risk Management Program eBook** for more details.

DOWNLOAD NOW

The Regulators

FFIEC
The Council is a formal interagency body empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions. FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions.

HHS
The Department of Health and Human Services' (HHS) Office for Civil Rights regulates the Health Insurance Portability and Accountability Act (HIPAA). Organizations covered by the HIPAA are required to protect personally identifiable information from fraud and theft, while also providing notification of breaches that impact protected health information.

FTC
The Federal Trade Commission (FTC) exists to protect consumer information and privacy by preventing business practices that are deemed fraudulent, deceptive, and unfair. The FTC's Safeguards Rule for consumer protection covers many entities. This independent agency also educates consumers on how to identify, stop, and prevent fraud and scams.

cfpb Consumer Financial Protection Bureau | FDIC | State Banking Commissions

Resources for Vendor Risk Management

Selected sources include:

- CFPB 2012-03 Service Providers Bulletin
- FDIC FIL-127-2008 Guidance on Payment Processor Relationships
- FDIC FIL-19-2019 Technology Service Provider Contracts
- FDIC FIL-23-2002 Country Risk Management
- FDIC FIL-121-2004 Computer Software Due Diligence
- FDIC FIL-27-2005 Guidance on Response Programs
- FDIC FIL-49-99 Bank Service Company Act
- FDIC FIL-44-2008 Third-Party Risk Guidance for Managing Third-Party Risk
- FDIC FIL-3-2012 Payment Processor Relationships
- Federal Reserve SR 13-19/CA 13-21 Guidance on Managing Outsourcing Risk
- FFIEC Information Technology Examination Handbook (esp. Appendix E)
- FFIEC Supervision of Technology Service Providers
- FFIEC Social Media: Consumer Compliance Risk Management Guidance
- FINRA Regulatory Notice 11-14
- FINRA Regulatory Notice 21-29
- FTC Safeguards Rule
- HIPAA Security Rule
- HIPAA Privacy Rule
- HITRUST CSF v9.6.0 License Agreement
- ISO/IEC 27001
- NCUA 08-CU-09 Evaluating Third-Party Relationships Questionnaire
- NCUA 07-CU-13 Evaluating Third-Party Relationships
- NCUA SL-17-01 Evaluating Compliance Risk - Updated Compliance Risk Indicators
- OCC-2013-29 Third-Party Relationships: Risk Management Guidance
- OCC-2017-7 Third-Party Relationships: Supplemental Examination Procedures
- OCC-2017-43 New, Modified, or Expanded Bank Products and Services: Risk Management Principles
- OCIE Cybersecurity and Resiliency Observations
- Payment Card Industry Data Security Standard (PCI-DSS)
- SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures
- SOC for Service Organizations: Information for Service Organizations

Continued Learning

Stay up-to-date with **Venminder's Resource Library** and **Third Party Thursdays Newsletter** (includes news, blogs, videos, podcasts, and more).

THIRD PARTY thinktank

Join **Third Party ThinkTank** -- a free online community for third-party risk management professionals.

Follow Venminder on **Twitter**, **LinkedIn**, and **Facebook**.

Contact us to learn more.

Download free samples of Venminder's vendor Control Assessments and see how they empower third-party risk professionals in mitigating risks.

DOWNLOAD NOW

PRINTABLE VERSION

venminder
Manage Vendors. Mitigate Risk. Reduce Workload.
+1 (888) 836-6463 | venminder.com