# 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** 



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.

timing, and approvals.



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

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.



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.

Your program document provides detailed information to senior management and

endor Risk Management Lifecycle

**Ongoing** 

Monitoring &

Performance

Governance Oversight & Accountability | Documentation & Reporting | Independent Review

Re-Assessments

Contracting

Due Diligence

**Due Diligence** 

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.

**DOCUMENTATION &** 

REPORTING

Perform a risk assessment to determine the inherent risk

and criticality of the vendor.

Inherent risk is naturally present

Renewals

**Termination** 

Exit Plan

Execution

**TPRM Closure** 

Offboarding

An internal or external

review from independent

auditors or third-party

assessors helps ensure

vour program complies

practices, or

certification standards.

requirements, best

with regulatory

The 3 Stages of

the Vendor Risk

Management

Lifecycle

**ONBOARDING** 

just at the beginning. A vendor's

risk and controls can change, so

scheduling a due diligence review

should occur in tandem with the

also be done before contract

at least annually is best. This review

risk re-assessment. Reviews should

**INDEPENDENT** 

**REVIEW** 



It's important

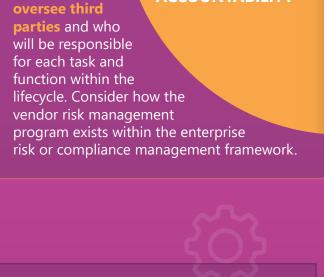
to understand

who will

Planning & Risk Assessment

**Onboarding** 

### **Three Essential Elements** of the Vendor Risk **Management Lifecycle**



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

of mitigating controls

the engagement's

and help you

determine

residual

validate the effectiveness

**OVERSIGHT &** 

**ACCOUNTABILITY** 

(remaining) risk. 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

use due diligence

vendor relationships,

assessment information

to determine whether any

contract provisions need to be added or re-negotiated.



**DUE DILIGENCE** 

**TERMINATION** 

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. Understanding the amount and types of vendor risk and validating vendor controls RISK ASSESSMENT

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

three years or before

low-risk vendors every two to





has changed enough to terminate the

**OFFBOARDING** 

Ending the vendor engagement

relationship.

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. **DUE DILIGENCE** 

**MONITORING &** 

**PERFORMANCE** 

**Contract** 

should be planned well in

advance, so you have

Subject Matter

FFIEC

**RENEWALS** 

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.



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** 

Who Is Involved?



**Regulatory Examiners** 

**Executive Leadership** and/or Board

Senior Management

## The Regulators

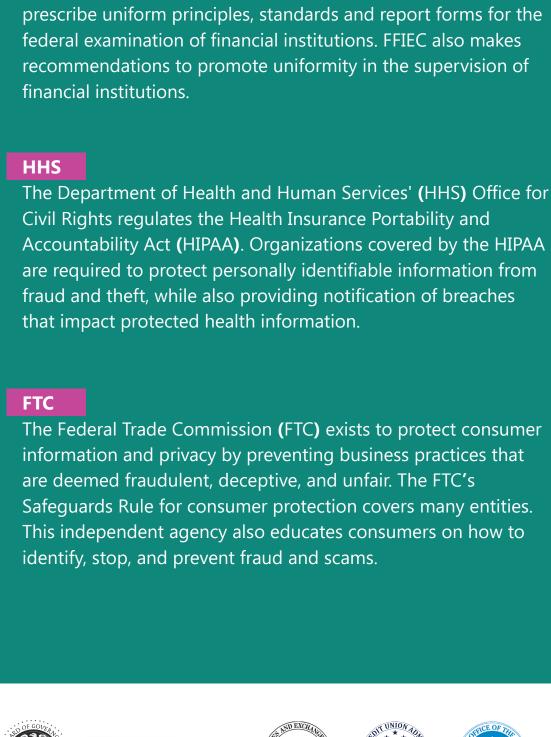
FFIEC

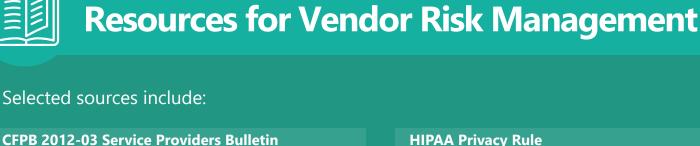
Download our Framework for a

**Program eBook** for more details.

**Successful Third-Party Risk Management** 

The Council is a formal interagency body empowered to





FDIC FIL-127-2008 Guidance on Payment

FDIC FIL-19-2019 Technology Service Provider

FDIC FIL-23-2002 Country Risk Management

**FDIC FIL-121-2004 Computer Software Due** 

FDIC FIL-27-2005 Guidance on Response

FDIC FIL-49-99 Bank Service Company Act

**FFIEC Social Media: Consumer Compliance Risk** 

**Processor Relationships** 

**Contracts** 

Diligence

**Programs** 

**Providers** 

**Management Guidance** 

**FTC Safeguards Rule** 

**HIPAA Security Rule** 

**FINRA Regulatory Notice 11-14** 

**FINRA Regulatory Notice 21-29** 

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 **Principles Managing Outsourcing Risk OCIE Cybersecurity and Resiliency FFIEC Information Technology Examination Observations Handbook (esp. Appendix E) Payment Card Industry Data Security Standard FFIEC Supervision of Technology Service** (PCI-DSS)

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

**Dedicated Vendor Auditors** Risk Management Team **Vendor Owners** 

**Third Parties** 

**DOWNLOAD NOW** 



**State Banking Commissions** 



and Facebook.

Download free samples of Venminder's vendor Control **Assessments** and see how they empower third-party risk







**Service Organizations** 

**HIPAA Privacy Rule** 

**ISO/IEC 27001** 

**HITRUST CSF v9.6.0 License Agreement** 



**SEC Commission Statement and Guidance on** 

**SOC for Service Organizations: Information for** 

**Public Company Cybersecurity Disclosures** 



Manage Vendors. Mitigate Risk. Reduce Workload.

+1 (888) 836-6463 | venminder.com

Contact us to learn more.

Join Third Party ThinkTank -- a free online community for third-party risk management professionals. Follow Venminder on Twitter, LinkedIn,



professionals in mitigating risks. **DOWNLOAD NOW** 

**PRINTABLE VERSION** 

Copyright © 2023 by Venminder, Inc.