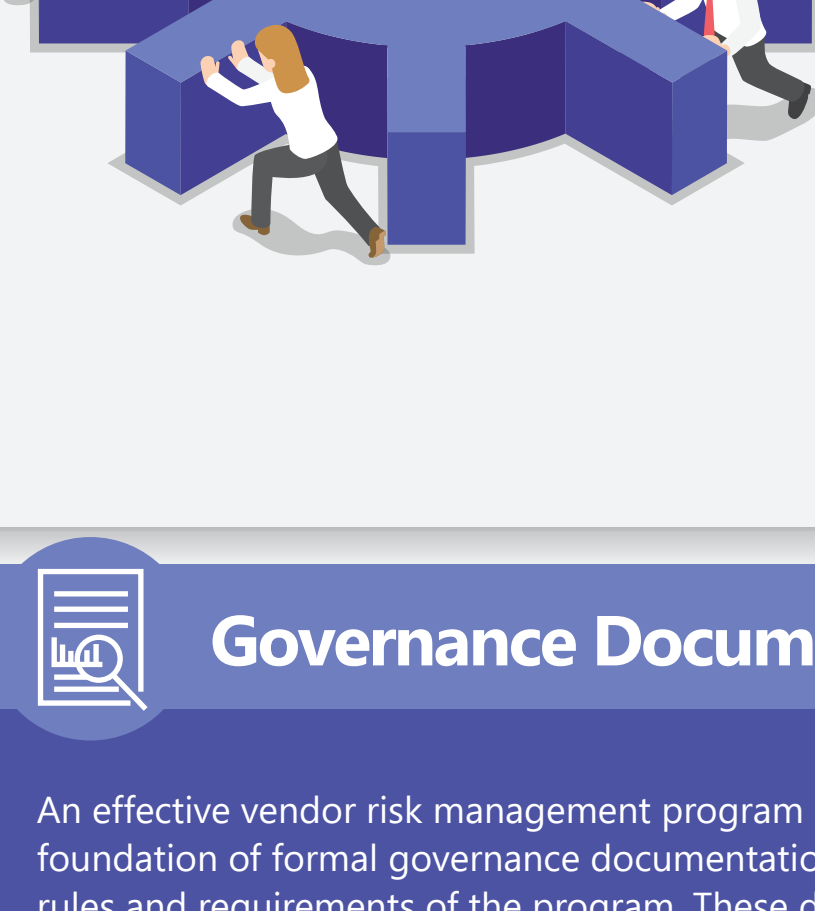


Vendor Risk Management Cheat Sheet

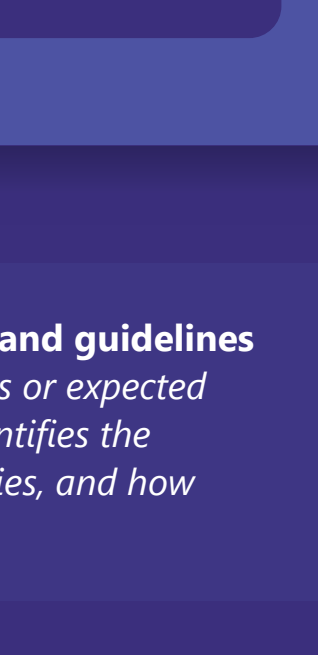


What Is Vendor Risk Management?

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.

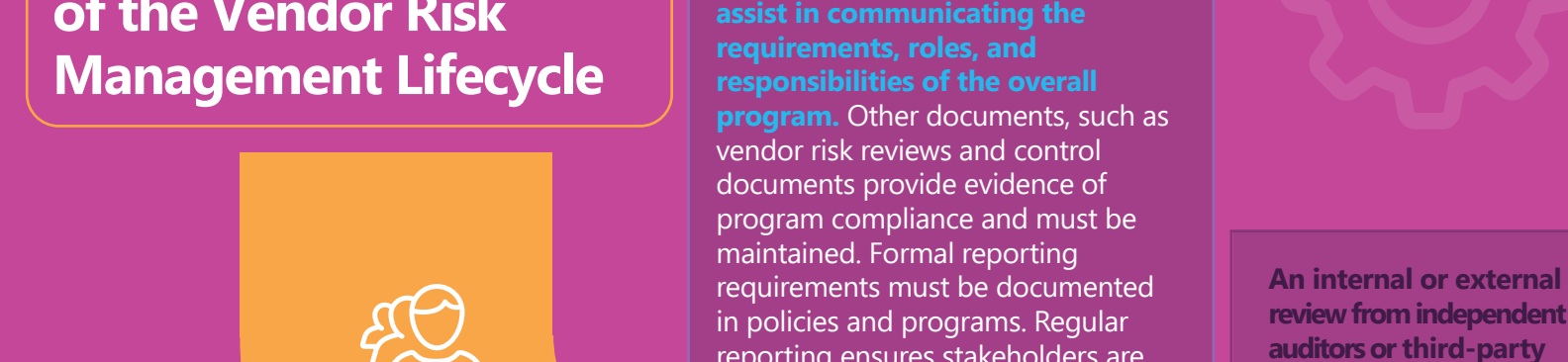
While all governance documents are important, you'll be asked to present your policy during an audit or regulatory exam. The policy should be reviewed and approved by the board (or senior management if there is no board) on an annual basis.

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.

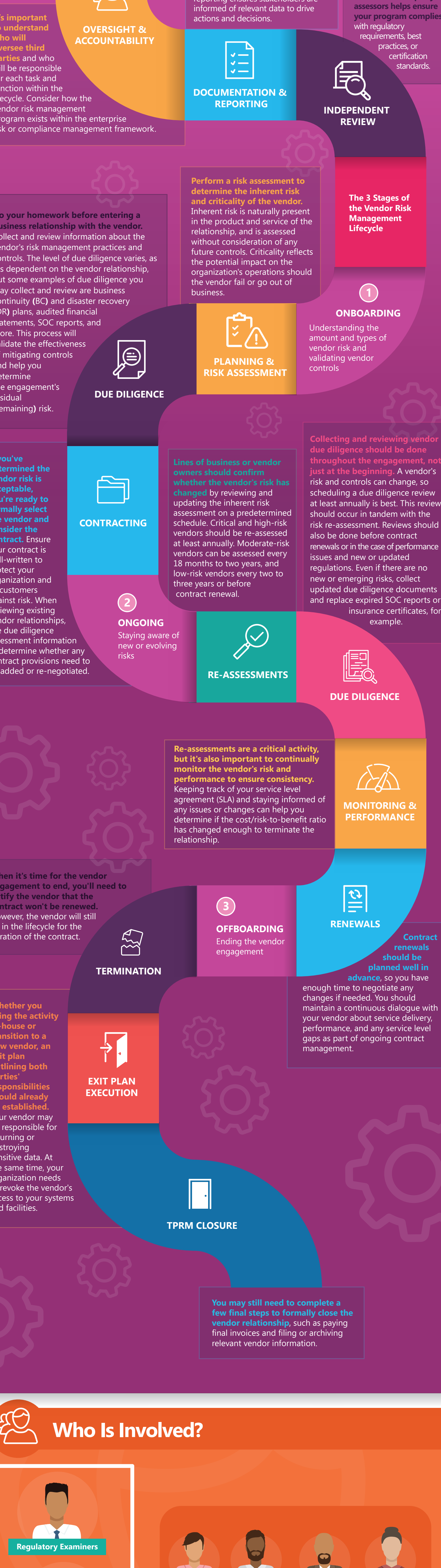


Procedures help ensure all tasks and activities are completed on time and correctly. Procedures can be reviewed and updated as necessary.

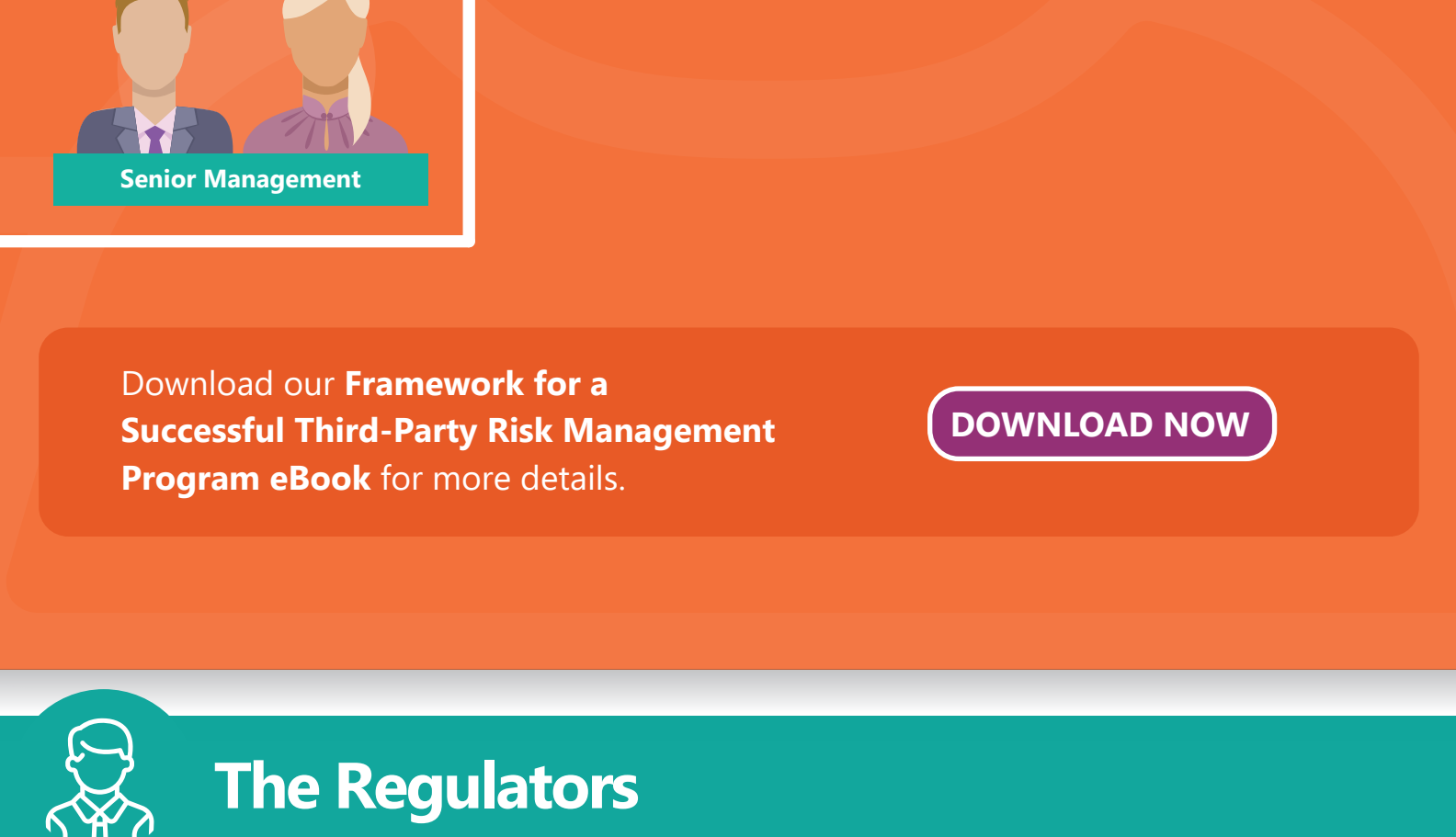
Vendor Risk Management Lifecycle



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



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 identifying 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.

Resources for Vendor Risk Management

Selected sources include:

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

Continued Learning

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

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](#)