Third-Party Risk Management Assessment

MARK NEU
CHIEF COMPLIANCE OFFICER
RENOWN HEALTH

Learning Objectives

- Scoping and buy-in of a TPRM Assessment tool
- Lessons earned
- One strategy for implementing the opportunities

AGENDA

Background

Selecting a TPRM Assessment framework

Fieldwork

Reporting

Implementing a TPRM program

Background

Internal Audit Risk Assessment completed for 2022/2023 Work Plan

Two of the nine Work Plan items contained some overlap of departments and processes

- *Cybersecurity Project*
- *Supply Chain – Source to Pay Assessment*

Proposed to combine both items for

- Auditor efficiency
- Auditee fatigue
- Management Action Plan efficiencies

Context

Evaluation of Corporate Compliance Programs (Updated March 2023), page 7
https://www.justice.gov/criminal-fraud/page/file/937501/download

Context - Evaluation of Corporate Compliance Programs

A well-designed compliance program should apply risk-based due diligence to its third-party relationships…

- …whether the company knows the business rationale for needing the third party in the transaction, and the risks posed by third-party partners
- …whether the company has ensured that contract terms with third parties specifically describe the services to be performed, that the third party is actually performing the work, and that its compensation is commensurate with the work being provided in that industry and geographical region
- …whether the company engaged in ongoing monitoring of the third-party relationships, be it through updated due diligence, training, audits, and/or annual compliance certifications by the third party

Context - Evaluation of Corporate Compliance Programs, continued

Consideration of Risk-Based and Integrated Processes

- How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company?
- How has this process been integrated into the relevant procurement and vendor management processes?

Context - Evaluation of Corporate Compliance Programs, continued

Consideration of Appropriate Controls

- How does the company ensure there is an appropriate business rationale for the use of third parties?
- If third parties were involved in the underlying misconduct, what was the business rationale for using those third parties?
- What mechanisms exist to ensure that the contract terms specifically describe the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?

Context - Evaluation of Corporate Compliance Programs, continued

Consideration of Management of Relationships

- How has the company considered and analyzed the compensation and incentive structures for third parties against compliance risks?
- How does the company monitor its third parties?
- Does the company have audit rights to analyze the books and accounts of third parties, and has the company exercised those rights in the past?
- How does the company train its third-party relationship manage about compliance risks and how to manage them?
- How does the company incentivize compliance and ethical behavior by third parties?
- Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?

Context - Evaluation of Corporate Compliance Programs, continued

Consideration of Real Actions and Consequences

- Does the company track red flags that are identified from due diligence of third parties and how those red flags are addressed?
- Does the company keep track of third parties that do not pass the company's due diligence or that are terminated, and does the company take steps to ensure that those third parties are not hired or re-hired at a later date?
- If third parties were involved in the misconduct at issue in the investigation, were red flags identified from the due diligence or after hiring the third party, and how were they resolved?
- Has a similar third-party been suspended, terminated, or audited as a result of compliance issues?

Selecting a TPRM Assessment Framework

VRMMM - Vendor Risk Management Maturity Model (Shared Assessments)

The VRMMM breaks third-party risk down into **eight** categories and explores more than **250** program elements that form the basis of a well-run third-party risk management program across the enterprise.

Foundation

1. Program Governance
2. Policies, Standards, Procedures
3. Contracts

Operations

4. Vendor Risk Assessment Process
5. Skills & Expertise
6. Communication & Information Sharing

Measurements

7. Tools, Measurement & Analysis
8. Monitoring & Review

Selecting a TPRM Assessment Framework

Example of Categorical Attributes and Criteria for *1.0 Program Governance*

Sub-Section # and Program Attribute
1.1 Risk Management Governance Model
1.2 Defined Program Objectives and Goals
1.3 Risk Management Strategy
1.4 Board Reporting and Management Oversight
1.5 ESG and Codes of Conduct
1.6 Mergers and Acquisitions

Sub-Section #	Attribute	Ques Num	Individual Detailed Criteria
1.1	Risk Management Governance Model	1.1.1	We define organizational structures that establish responsibility and accountability for the oversight of our vendor relationships.
		1.1.2	The organizational structure of our vendor risk management program operates independently of our business lines.
		1.1.3	We have established a formal program review schedule to conduct periodic self-assessments of program maturity.
		1.1.4	We have defined specific requirements for engaging vendors based on the scope of service and product specifications.
		1.1.4.1	We have defined specific requirements for vendor and business partner engagements based on type of outsourcing.
		1.1.4.2	We have defined service level agreements as required for vendor and business partner engagements based on type of outsourcing.
		1.1.5	We have defined specific requirements for roles and responsibilities for functions that perform vendor risk management activities.
		1.1.6	We have defined the criteria for conducting independent assessments to evaluate the program's effectiveness.
		1.1.7	We have included the vendor risk management program as a component of our enterprise risk management program.

Fieldwork

- Supply Chain
- Legal
- Information Security
- Compliance
- Health Plan – Note the Medicare Advantage requirements for First-tier, Downstream, and Related entities (FDRs)
- Reliable Data, Reliable Data, Reliable Data

Reporting

- Draft Report V1, V2, V3…
- Be mindful of “Audit” versus “Assessment”, and similarly “Opportunities” not “Risks” and “Findings”
- One-dozen eggs or 12 eggs?

Implementing a TPRM program

What to do with the results

- Re-tooled the existing Governance, Risk and Compliance (GRC) Committee
- Attended by all key stakeholders
- GRC reports up to the Audit and Compliance Committee
- Translated the results into a GRC Work Plan

Wrap-up

What would we have done differently?

- Ensure organizational standards and processes are codified.
- Been more intentional about the VRMMM tool/detail at the opening meeting
- Been more thoughtful of Assessment owner at the opening meeting
- Overcommunicated Assessment versus Audit

Speaker contact info

Mark Neu, MHA, CHC, CCEP

mark.neu@renown.org

775.982-5596