COHN REZNICK
ACCOUNTING • TAX • ADVISORY

GOVERNANCE, RISK, AND COMPLIANCE *INSIGHTS*

Forward Thinking Thought Leadership

How to Manage Third-Party Risk to an Organization

Risk is an ever-moving, ever-evolving target that takes on many forms—data breach, negative public opinion, security breakdown, business operations failure, regulatory violation, government intervention, and copyright law, to name a few. Reputational harm and litigation that can result from such manifestations of risk take years to overcome. Delayed service delivery and product disruption—another potential consequence of poorly managed risk areas—negatively affect revenue. Today, many companies rely on outside service providers to make their business succeed and remain competitive. Commonly outsourced business operations include:

- Payroll and Employee Benefits
- Data Center
- Call Center Operations
- Software Partners
- Offshore Manufacturers
- Billing Services
- Cloud Service Provider
- Email Provider
- Hardware Providers
- Offsite Storage

While internal business activities present a level of risk, the organization's third-party relationships make overall risk management especially challenging. Some companies do not have in-house risk management or compliance groups, and the responsibility of managing third-party risk sometimes gets lost.

QUESTIONS INTERNAL AUDIT SHOULD ASK

1. Are third-party risks considered with the company's risk appetite and overall approach to enterprise risk management?
2. Have third-party risks been identified and ranked?
3. Are third-party risk management roles and responsibilities defined?
4. Does the organization have appropriate resources to adequately address third-party risk?
5. Is Internal Audit effectively considering third-party risk within their risk assessment and internal audit plan?

Establishing a Third-Party Risk Management Program

Building a new third-party risk management program is an immense undertaking. It is imperative that senior management sponsor the program, assign an effective cross-functional team that will help drive accountability throughout the organization, and provide sufficient resources to effectively carry out an effective third-party risk management program. With adequate sponsorship and resources, the third-party risk management program can be developed and implemented throughout the organization through these five steps:

1. **Set Governance:** Formalize an enterprise third-party risk management governance structure with defined roles and responsibilities across the organization
2. **Determine Relationship Risk:** Maintain an accurate and complete inventory of third-parties and the respective relationship risks
3. **Manage Risk:** Establish risk stratification, due diligence, and monitoring methodologies and policies to manage each third-party relationship
4. **Control Validation:** Validate controls at the third party and ensure the program adapts to changes with the third party's risk profile
5. **Monitor and Report:** Use integrated technology platform and MIS workflow to support the TPRM program

Who Should Own Third-Party Risk?

Carrying out these guiding principles and ensuring the company's risk exposure is adequately addressed often falls to enterprise risk management and internal audit. However, this responsibility should fall to multiple stakeholders of the organization—from various business units, to subject matter specialists in procurement, legal, risk, finance, and technology.

These key stakeholders should establish the necessary controls and procedures to minimize risks, while internal audit can provide an objective assessment of the controls, recommend improvements, and offer assurance to management and the board that third-party risk is addressed appropriately. The bottom line is that organizations must assign ownership of third-party risk to a dedicated, qualified team or external group, then provide necessary supporting resources.

COHN REZNICK
ACCOUNTING • TAX • ADVISORY

Key Stakeholder Responsibilities

Internal Audit
- Provides assurance on the effectiveness of governance, risk management, and controls, including third-party risk management
- Acts with recognized standards and reports to high level within the organization

Enterprise Risk Management
- Sets risk tolernance levels for the organization
- Monitors and enforces overall risk policy

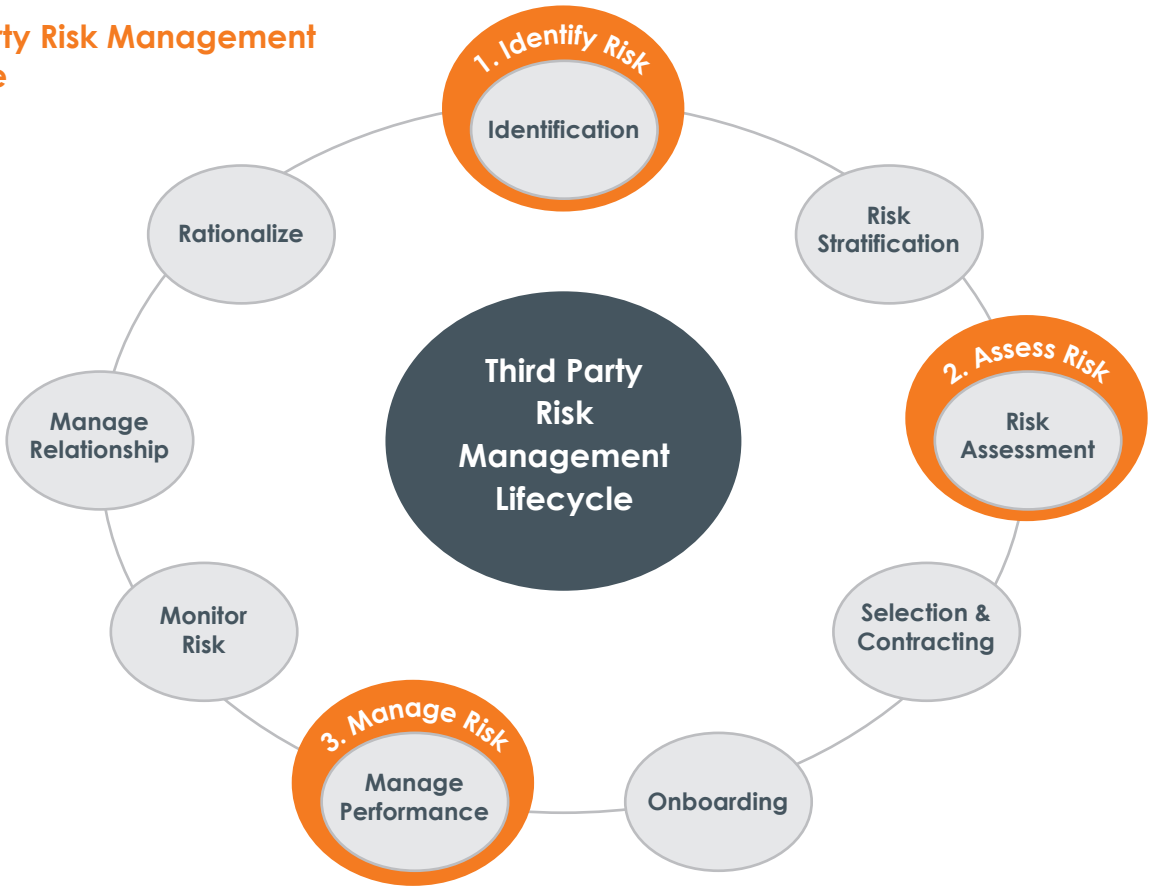
Legal/Sourcing
- Supports contract negotiation, pricing ,and SLAs
- Monitors contract risk and compliance
- Consults on laws and regulations
- Responsible for due diligence, reference checks, selection
- Spend reporting

Third-Party Risk Management
- Establishes third-party risk policies, principles, and tolerances
- Manages overall third-party relationships
- Coordinates TPRM program to all stakeholders
- Monitors business health of the third party
- Ensures third-party meets risk policies
- Ensures third-party risk assessments and necessary audits are performed
- Rationalizes the vendor's value

Information Security
- Standardizes and automates risk reporting and monitoring
- Supports due diligence efforts
- Enforces and validates security standards and improvements by the third party

Business Owners
- Manages the risk of third-party
- Monitors day-to-day third-party operations
- Ensures speed in contracting process
- Escalates any issues and concerns

Third-Party Risk Management Lifecycle



Management Strategy	Policies and Procedures	Program Governance	Technology Platform/MIS

ORGANIZATIONAL GOVERNANCE, PRINCIPLES, AND FRAMEWORK

Benefits to Formalizing a Third-Party Management Function

QUALITY

- Higher quality of third-party risk management throughout the third-party lifecycle
- Tighter controls and increased accountability over third parties that pose significant risk

STANDARDIZATION

- Streamlined and standardized processes for third-party onboarding, risk profiling, and ongoing monitoring and ove
- Improved quality, efficiency, timeliness, and accuracy of third-party risk management, from workflow and reporting tools
- Greater benefits realized from scorecards and dashboards through use of standardized KPIs and KRIs

RISK

- More effective monitoring of due diligence activities and their frequency, driven by both inherent and residual risks
- Greater agility in responding to changing regulatory requirements and other third-party risk management challenges

FLEXIBILITY AND EFFICIENCY

- Tight focus on controls associated with those relationships found to pose the greatest risk, through third-party stratification
- Ability to redirect the efforts of staff based on identified organizational priorit
- Enhanced ability to quickly undertake new initiatives and locate third-party replacements more rapidly

STAKEHOLDER VALUE

- Ability to rationalize the value of the third-party and its service to the organization
- Improved compliance with federal laws and regulations and reduction of fines or penalties that may impact the bottom line
- Appropriately trained and placed resources

Best Practice Key Takeaways

Recent breaches, business failures, and other security incidents prove that the implementation of a third-party risk management program is essential. Recent breaches, business failures, and other security incidents prove that the implementation of a third-party risk management program is essential. Organizations must understand the risk of each third party and how to effectively manage and mitigate that risk. Several key steps can help organizations accomplish these tasks:

About CohnReznick's Governance, Risk, and Compliance Practice

CohnReznick's Governance, Risk, and Compliance (GRC) Practice provides boards of directors and senior management of public, private, and not-for-profit organizations with the experience, objectivity, and resources they need to meet their governance, risk, and compliance responsibilities—and to leverage the insight these activities generate to improve operations, enhance value, and ultimately help realize the organization's missions.

Contact

For more information on how to prepare for the transition to the new lease accounting standard and avoid implementation challenges, please contact:

George Gallinger
Principal
CohnReznick Advisory
George.Gallinger@cohnreznick.com
973-871-4060

Daniel Fornelius
Senior Manager
CohnReznick Advisory
Daniel.Fornelius@cohnreznick.com
973-871-4037

To learn more about CohnReznick Advisory's Government, Risk, and Compliance Practice, visit www.cohnreznick.com/services/advisory/governance-risk-and-compliance.

May 2017