The Need for an Integrated Approach to Manage Third Party Risk

DRIC 2024 Spring Symposium

April 11, 2024

Introduction

Phil Racco

Senior Manager
Enterprise Risk Services

philip.racco@mnp.ca

Deepak Jaswal

Senior Manager
Enterprise Risk Services

deepak.jaswal@mnp.ca

Background

01

Ever-Expanding Third-Party Network

Continued use of and reliance on third parties has heightened existing risks and highlighted new areas of exposure.

02

A Third Parties Risks Become Your Risks

From data breaches to operational disruption, from compliance to reputational damage, a third parties' risks do not stay their own, and managing these exposures has become more important than ever.

03

A Need for a Better Approach

A more sophisticated and integrated approach to evaluating potential threats stemming from the use of vendors, affiliates and other external parties is becoming a necessity for all organizations.

Objectives

01 Increase understanding of third-party risk, including sources, exposures, and potential impacts/implications

02 Provide an overview of third-party risk management, including the third-party lifecycle, programs, and tools

03 Discuss the need for a diverse and integrated approach to third-party risk management

Agenda

Introductions	*5 mins*
Defining Third-Party Risk	*10 mins*
Walkthrough of the Third-Party Risk Management & the Lifecycle	*15 mins*
The Call for an Integrated Approach	*15 mins*
Questions & Wrap Up	*15 mins*

Defining Third Party Risk

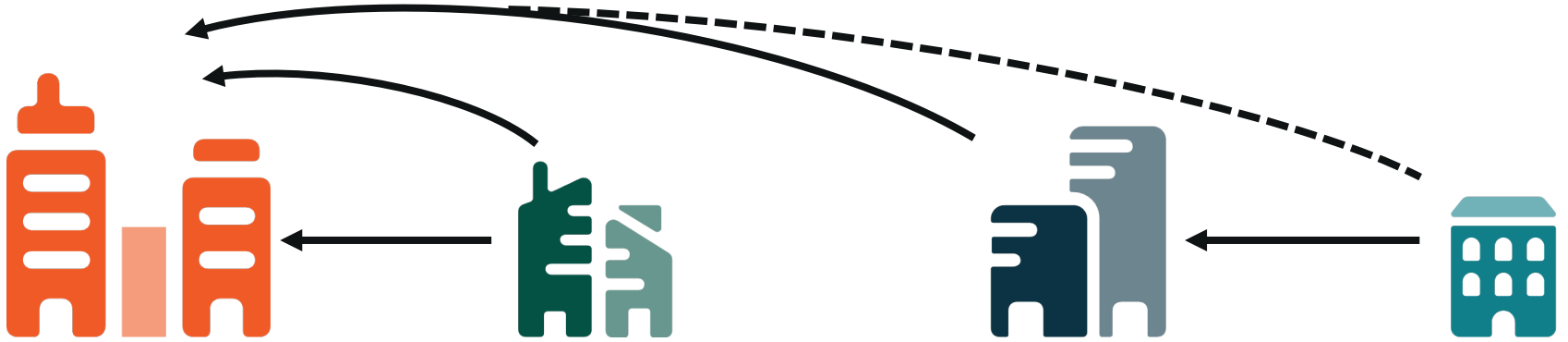
Increase understanding of third-party risk, including sources, exposures, and potential impacts/implications

What is a Third Party?

Any entity or person that works on behalf of an organization, or is being considered for such a role, but is ***not an employee***, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates/partners, and any other person. *A third-party may itself have organizations performing work on behalf of a first-party*. The term may have specific meaning within the context of individual regulations.

Adapted from: Shared Assessment

Relationships & Parties



The First Party	The Second Party	The Third Party	Nth Party
The First Party (or Outsourcer) is the entity delegating a function to another entity.	The Second Party is related party of the First Party (e.g., a subsidiary or parent company).	The Third Party is the entity that performs the work on behalf of the First Party. The Third Party is always separate from the First Party.	The Nth Party (also known as the Subcontractor) is an entity independent of and directly performing tasks for the Third Party, working on behalf of the Third Party to deliver services to the First Party.

Adapted from: Shared Assessment

What is Third-Party Risk?

Potential *threats stemming* from the *use of vendors, affiliates, partners and other external parties* that support a first party.

Third-party risks can have a *variety of implications*:

- Operational
- Compliance
- Legal
- Financial
- Reputation
- People

Adapted from: Shared Assessment

Notable Examples

Termination of 'Yeezy' brand due to antisemitic comments by Kanye West.

Ransomware attack and the resulting data breach, impacting over 13,000 business customers.

Production disruption due to a supplier cyber attack.

Data breach to a vendor resulted in compromised customer data.

Unauthorized access to systems, impacting credit union clients.

An Overview of Third-Party Risk Management

Provide an overview of third-party risk management, including the third-party lifecycle, programs, and tools

What is Third Party Risk Management?

Evaluating and compensating for potential threats stemming from the use of third parties (e.g., vendors, affiliates, partners and other external parties) that support an organization.

Third Party Risk Management (TPRM) comprises the various actions an organization undertakes to manage its use of third parties across the *Third-Party Risk Management Lifecycle*.

Adapted from: Shared Assessment

Third-Party Risk Management Lifecycle

Identification & Due Diligence

Contracting & Onboarding

Performance Monitoring

Evaluation

Offboarding / Renewal

Identification & Due Diligence

Purpose

Identify and understand the third party we are looking to engage.

Key Activities & Considerations

- Define the requirements of the third-party
- Understand the people, processes and technology required to deliver services
- Perform research on the entity (e.g., financial stability, reputation, legal relationships, control environment, social posture, etc.)
- Analyze the potential risk exposure

Identification & Due Diligence

Some factors and considerations for criticality

Organizational Structure

Data (Type & Access)

Availability of Alternates

Risk Management Practices

Size of Contractual Expenditure

Jurisdiction(s)

Contracting & Onboarding

Purpose

Establish a platform for success in managing the third-party relationship.

Key Activities & Considerations

- Establish:
  - Service standards – and other rights – defined inside of contract
  - Rules or limitations to subcontracting
  - Ownership and access to assets generated
  - Offboarding process
- Onboard the third party to assist with change management

Performance Monitoring

Purpose

Ongoing oversight of the third-party against desired outcomes.

Key Activities & Considerations

- Monitoring of SLAs/KPIs
- Completion of analysis via audits or questionnaires
- Review of assurance reports
- Reporting to management and oversight bodies on performance

Evaluation

Purpose

With term completed (or pending renewal), determine the effectiveness of the relationship.

Key Activities & Considerations

- Review and grading of overall relationship and value realization
- Changes in third-party criticality and/or services required
- Costs
- Regulatory changes

Offboarding / Renewal

Purpose

Ensure continuity of outcomes, via renewal or with a new party.

Key Activities & Considerations

- Establish renewal or transition plan
- Update or end contract
- Update third-party database (and blacklist if necessary)

The Need for a Different Approach

Discuss the need for a diverse and integrated approach to third-party risk management

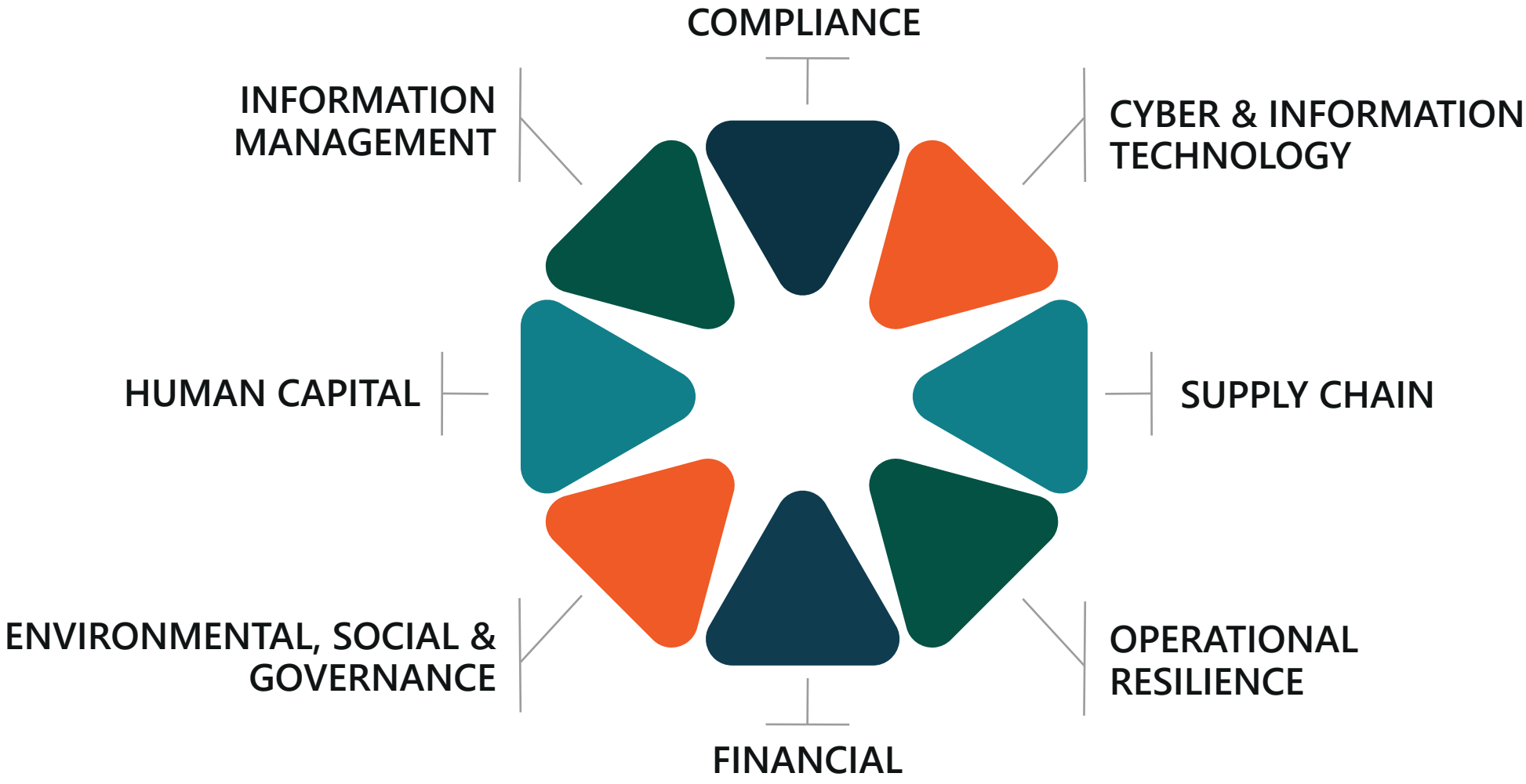
Gaps in Current Approaches

Generally, organizations tend take a disparate approach to managing third parties:

- Narrow definition of third parties.
- No clear governance of third parties.
- Disconnected / unaligned processes and tools.
- Ineffective data and reporting.

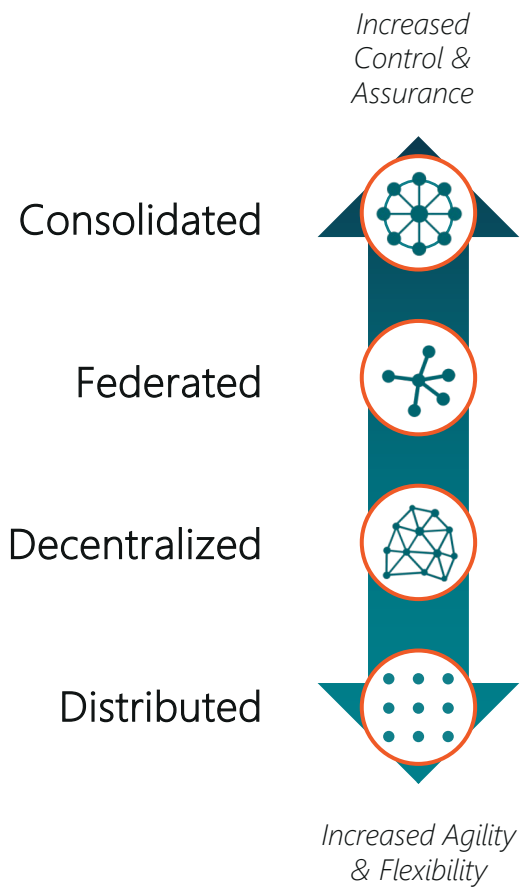
The goal must be to manage the third party *across the organization throughout the entire lifecycle*.

The Goal: Diversity & Integration



Form & Function Will Vary

- Risk programs can take a variety of forms, which will influence how an organization approaches risk in general (and third-party risk specifically)
- To ensure appropriate outcomes are reached, focus should be placed less on form and more on function



A Framework to Assess Programs

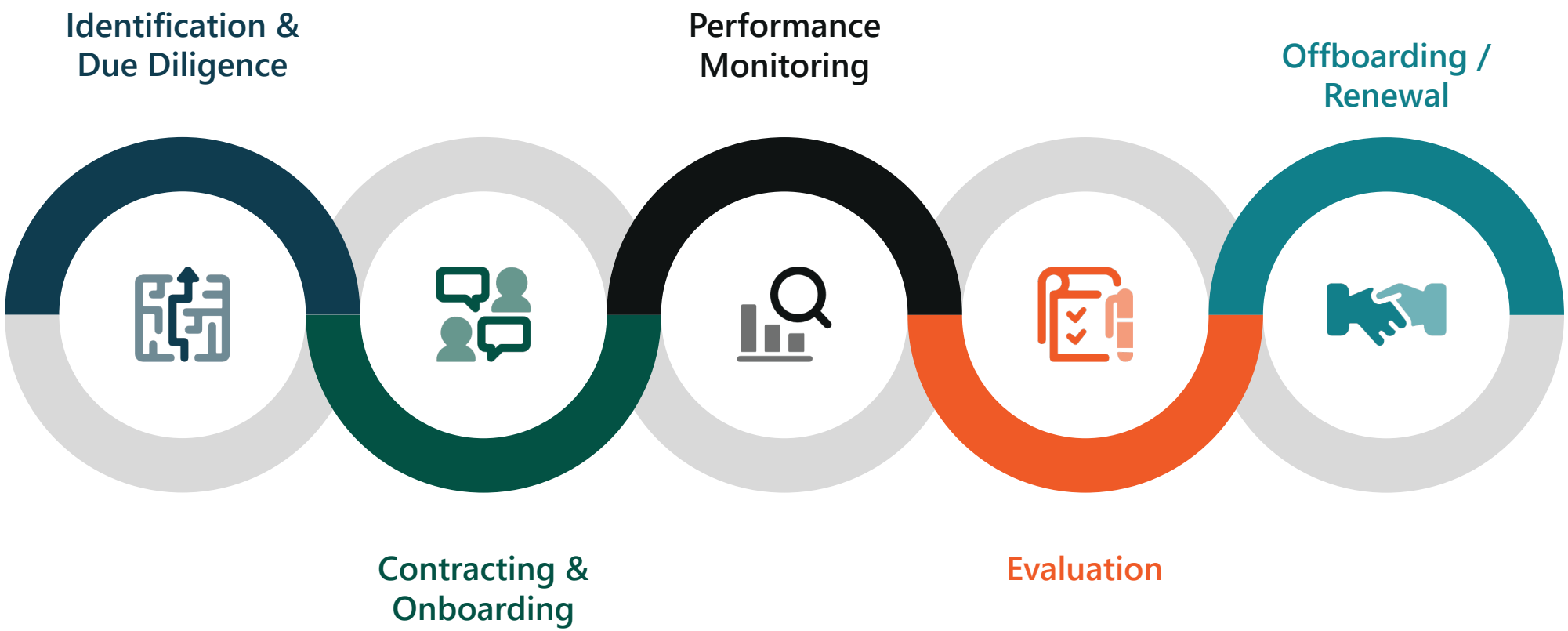
- When we are asked to look at a risk program, we consider nine (9) elements across three (3) categories
- Using this lens to identify how and when a program can be integrated to better manage third party exposures

Category	Element
Design	Governance & Strategy Policy, Framework & Tools Risk Appetite
Operationalization	Lifecycle People & Skillsets Reporting & Communications
Outcomes	Culture Decision-Making Monitoring & Improvement

Linkage Between TPRM and BCM

- The need to consider the implications of third parties for operational resilience is obvious
  - Data and privacy
  - Cybersecurity
  - Supply chain
  - Continuity of processes/services
- The issue is the manner by which BCM efforts can effectively help to manage third party risk exposures

BCM Across the TPRM Lifecycle



Wrap Up

Some final thoughts and time for questions

Final Thoughts

- Third party risk is ever present and will continue to evolve
- BCM has always factored in the risk from third parties, but there is opportunity for a more holistic approach
- There is no 'one size fits all' method, but there is a need for an organization to take an integrated approach considering a diversity of factors (including its risk appetite)
- Effective management of third parties will take adjustments to people, processes, and systems

Questions?

Thank you

Deepak Jaswal
Senior Manager, ERS
deepak.jaswal@mnp.ca

Phil Racco
Senior Manager, ERS
philip.racco@mnp.ca


MNP
MNP
MNP
Wherever business takes you
MNP.ca
PRAXITY
Empowering Business Globally