Third-Party Risk Management

Reducing the Cost of Third-Party Compliance

Preview Report

CEB Compliance & Ethics Leadership Council

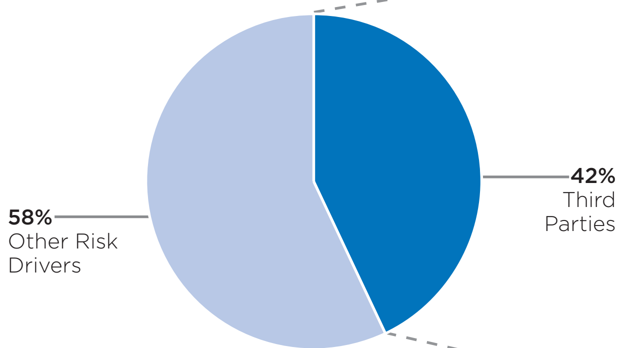
WHAT THE BEST COMPANIES DO

Third parties act as contributing parties or exacerbating factors to all forms of compliance risk.

THIRD PARTIES MAGNIFY COMPLIANCE RISK

Third Parties Drive Compliance Risk Exposure

Percentage of Risk Exposure Compliance Executives Attribute to Third Parties



Select Examples of Third-Party Risk

Bribery and Corruption

91% of FCPA cases between 2011 and 2014 involved third parties.[4]

Data Privacy

- 36% of 2014 corporate data breaches involved third parties.
- Third party involvement increased the average cost per breach by $721,175.[5]

Reputation Risk

- Only 47% of executives feel prepared to manage the reputational risk created by third parties.[6]

n = 47.

Source: CEB 2015 Third-Party Risk Diagnostic.

[4] CEB Settlements Analysis.

[5] Ponemon Institute, 2014 Cost of Data Breach Study.

[6] Tatiana Serafin, "Reputation Risk Leading Company Concern in 2015," Forbes (January 2015), http://www.forbes.com/sites/tatianaserafin/2015/01/05/reputation-risk-leading-company-concern-in-2015/.

Third-Party Factors That Magnify Risk

1 **Control Gaps**

2 **Increased Touchpoints**

3 **Misaligned Incentives**

AN OPERATING TAX

The Cost of Third-Party Compliance
Estimated Cost of Each Activity, per Year

Compliance Costs		Business Costs	
20%	**Compliance Time Spent Managing Third-Party Risk**	18,000	**Business Days Spent Waiting for Third-Party Approval**[a]
28%	**Compliance Budget Spent Managing Third-Party Risk**	$525,000	**Annual Due Diligence Spend**[b]

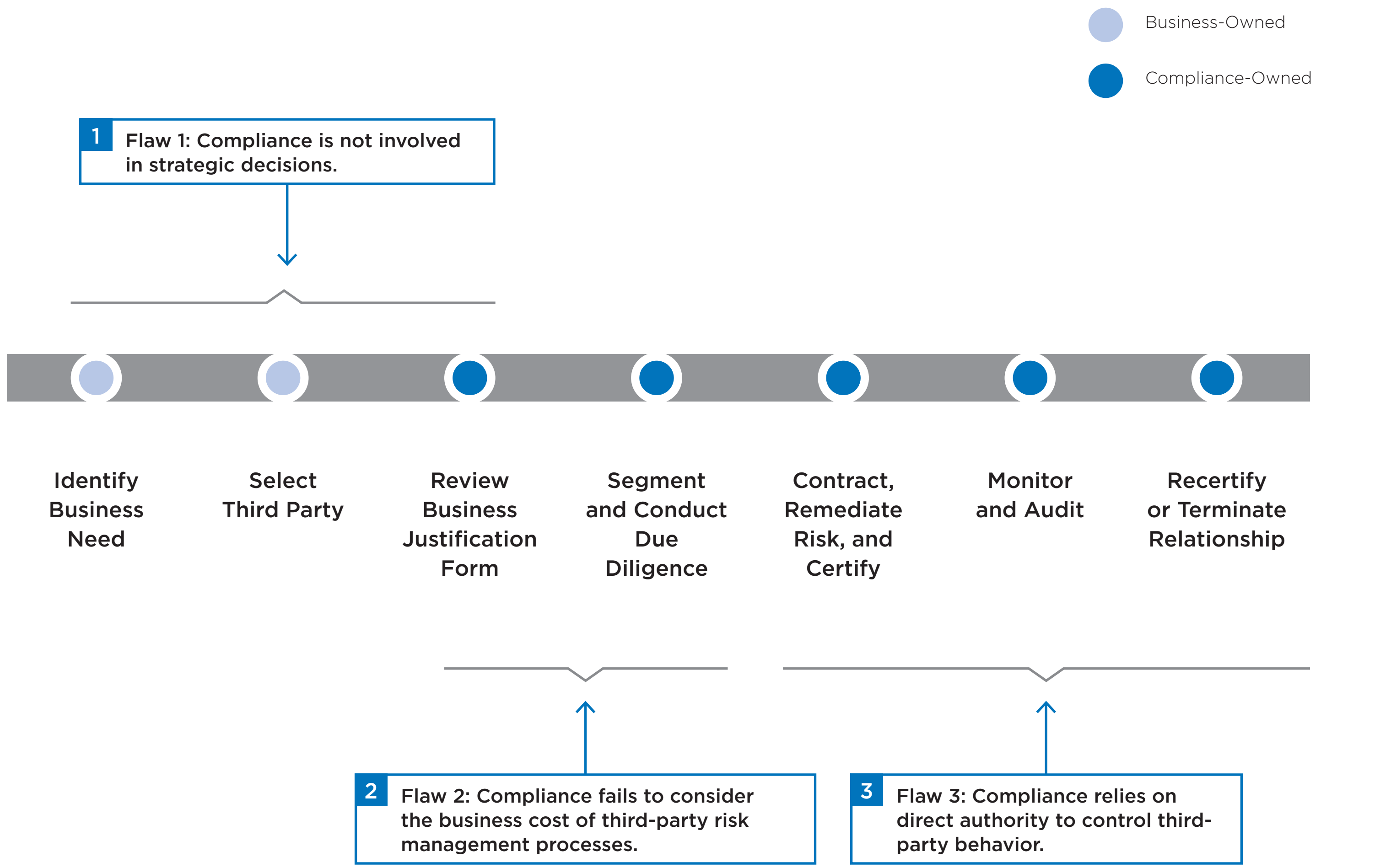
n = 55–82.
Source: CEB 2015 Third-Party Risk Diagnostic.
[a] 18,000 = 60-day median cycle time x 300 estimated number of new third parties receiving due diligence in a given year.
[b] $525,000 = Basic Due Diligence ($250 estimated charge of basic due diligence per third party x 300 estimated number of third parties that receive due diligence) + Enhanced Due Diligence ($15,000 estimated charge for enhanced due diligence x 30 estimated number of third parties that receive enhanced due diligence).

Undercutting the Advantage
The dual costs of increased risk exposure and an expensive management process undermine the business rationale for using third parties.

There are three fundamental flaws in Compliance's current approach to third-party risk management.

WHERE WE GO WRONG

Failure Points in Enforcing Standards for Third-Party Behavior



Source: CEB analysis.

Compliance can address these flaws by taking a Business Accelerator approach to third-party risk management.

A BETTER ROLE FOR COMPLIANCE

Key Differences Between the Policy Enforcer and the Business Accelerator Approaches

	Policy Enforcer (Current Approach)	Business Accelerator Approach
Working Assumption	Compliance standards influence behavior.	Time and cost considerations influence behavior.
Resulting Strategy	**Tell Business Stakeholders What to Do** Establish and enforce compliance standards for third-party behavior.	**Help Business Stakeholders Make Informed Decisions** Partner with business stakeholders (i.e., internal business sponsors, third parties) to improve compliance decisions and streamline processes.

Best-in-class Business Accelerators achieve greater process adherence and influence over business decisions than best-in-class Policy Enforcers.

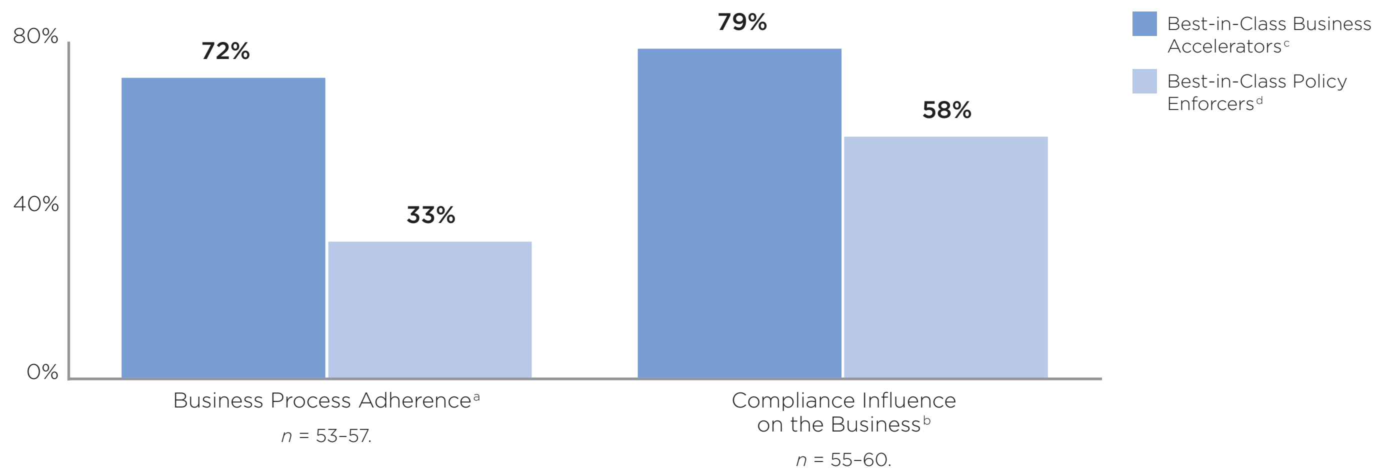
BUSINESS ACCELERATORS ACHIEVE GREATER RISK REDUCTION...

Business Accelerators are More Confident in Process Adherence and Compliance Influence

Percentage of Respondents Agreeing or Strongly Agreeing

Reducing Risk

Business Accelerators improve the internal oversight of third-party behavior.



Source: CEB 2015 Third-Party Risk Diagnostic.

[a] Index of percent selecting never or almost never when asked "How often do internal partners avoid the compliance review process?" and percent selecting always or almost always when asked, "How often are compliance recommendations followed?"

[b] Index of percent agreeing and strongly agreeing with these statements: "Business partners seek guidance from the compliance ethics program about how to best reduce third-party risk to the organization" and "Business partners act on the third-party information provided by the compliance and ethics program."

[c] Top quartile performance against the Business Accelerator Index.

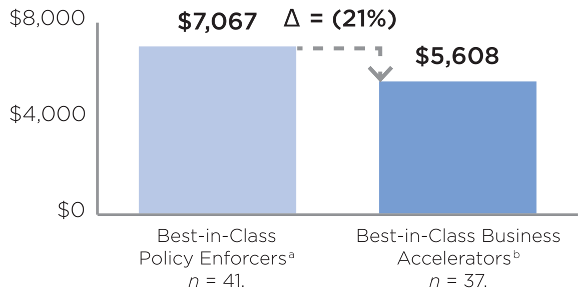
[d] Top quartile performance against the Policy Enforcer Index.

Business Accelerators spend less money and time on third-party risk management.

...AT LESS COST

Strong Business Accelerators Spend Less Money...

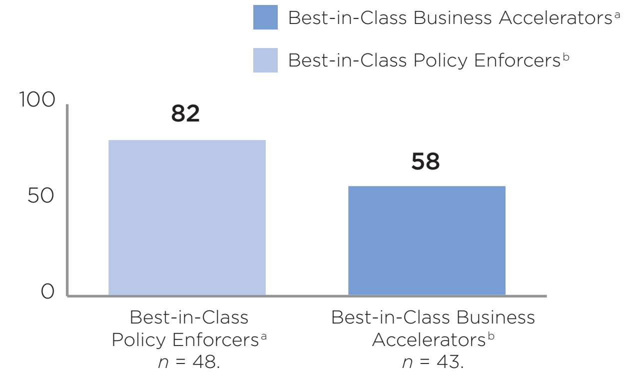
Median Spend on Third Parties, Per 100 Third Parties



Source: CEB 2015 Third-Party Risk Diagnostic.

...and Process Third Parties Faster.

Mean Compliance Time Spent Reviewing Third Parties, in Business Days



Source: CEB 2015 Third-Party Risk Diagnostic.

24 Days	x	300	=	7,200 Days
Difference in Compliance Time Spent Reviewing Third Parties		Estimated Number of Third Parties Receiving Due Diligence, Per Year		Best-in-Class Business Accelerator Annual Time Saved

Source: CEB 2015 Third-Party Risk Diagnostic.

[a] Top quartile performance against the Business Accelerator Index.

[b] Top quartile performance against the Policy Enforcer Index.

Profile of a Best-in-Class Business Accelerator:

- At companies with median FTE size of 24,000
- Work with 5,572 third parties
- Spend 19% of the program's budget on third-party risk management
- Spend 23% of the program's time on third-party risk management

Business Accelerators achieve these outcomes by employing three strategies.

THE PATH FORWARD

Key Business Accelerator Strategies

How Do Business Accelerators Achieve Greater Risk Reduction at Less Cost?

Make Third-Party Cost Transparent

1. Create incentives for internal partners to consider third-party risk.
2. Support the initial selection of potential third parties.
3. Obtain business buy-in and support for third-party management.

Reduce the Business Cost of Compliance

1. Ensure the flow of third-party information to internal stakeholders.
2. Build internal capability for managing third-party compliance risk.
3. Prioritize solutions-orientation.

Harness Third-Party Self-Interest

1. Focus segmentation on the identification of specific risks to be managed.
2. Build incentives for third parties to improve their compliance programs.
3. Map third-party management support to capability gaps.

What Doesn't Matter:

- Compliance and Ethics primarily focuses on enforcing third-party adherence to its standards, requirements, and controls.
- Compliance and Ethics can most effectively reduce third-party risk by getting the business to accept heightened due diligence on third parties.
- Reports on third-party due diligence, certifications, and attestations help the business better manage third-party risk.

"There are two basic signs of success: Are we able to add third parties without adding more risk, and are we able to do this while continuing to operate efficiently?"

Benjamin Bard
Vice President, Global Chief Compliance Officer
Archer Daniels Midland Company

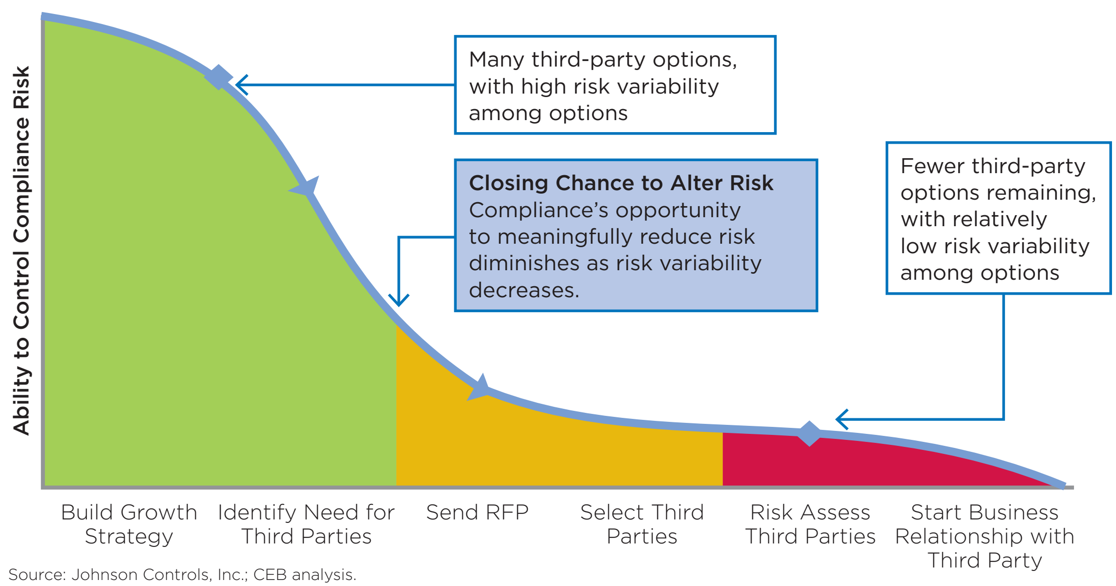
As the procurement process progresses, the risk variability among prospective third parties decreases.

- Compliance programs typically get involved in risk assessing third parties after they have been selected, limiting total possible risk reduction.
- Early involvement allows Compliance to consider a broader group of third parties and path the business toward the options with the best risk-reward tradeoff.

A CLOSING WINDOW

Ability to Control Risk Decreases Throughout the Procurement Process

Risk Variability Among Prospective Third Parties, Illustrative



Source: Johnson Controls, Inc.; CEB analysis.

Key Elements of Johnson Controls' Early Strategic Decision Support

1 **Uncover Third-Party Options**
Ask questions of business partners that uncover information about upcoming business initiatives and reveal untested assumptions about how the business should work with third parties.

2 **Provide a Complete Cost-Benefit Analysis**
Price the risk and remediation costs of working with third parties so that the business understands the full costs of working with third parties.

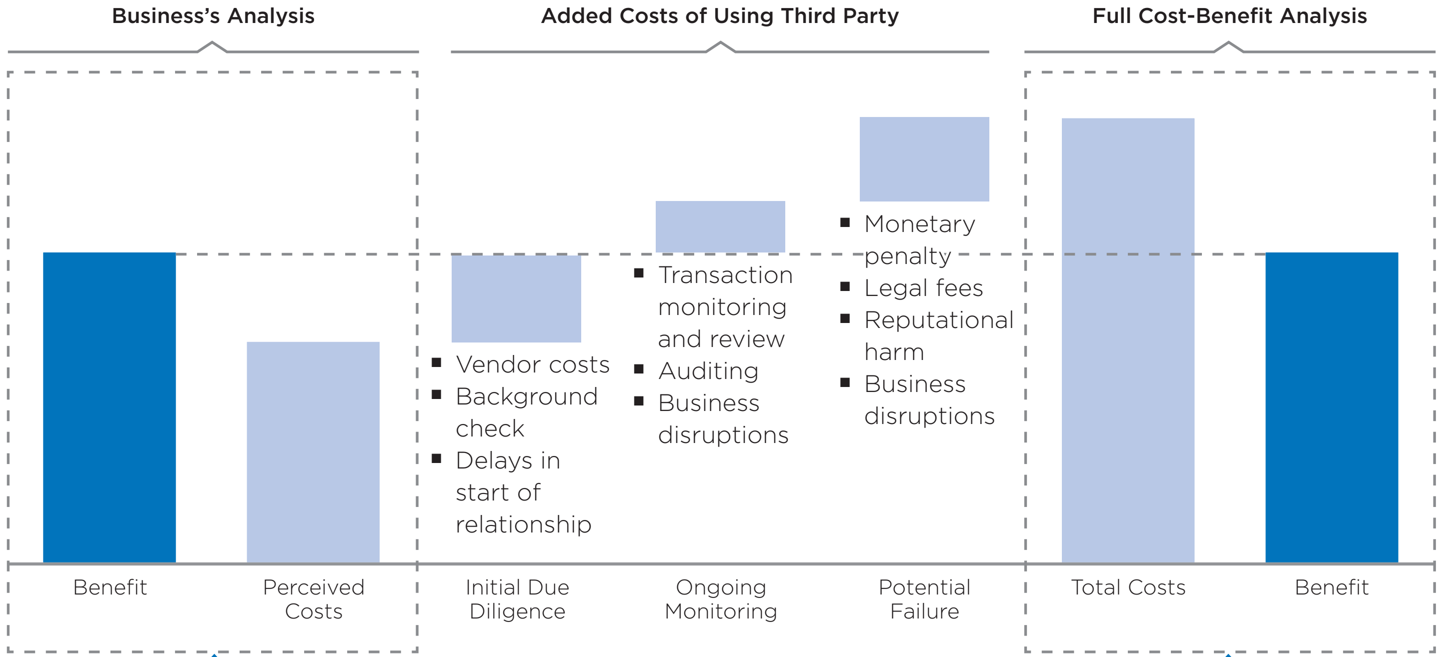
Compliance creates value by offering the business a more accurate cost-benefit analysis that incorporates compliance-related costs.

- Most compliance programs assume that the business won't be receptive to their input on strategy because they underestimate the value they can add through their expertise.
- Once business partners see how Compliance can add value by pricing risk management, they become more receptive to Compliance's perspective in future strategic discussions.
- Compliance helps the business avoid risk in third-party options only if it moves towards early strategic decisions.

PROVIDING A MORE ACCURATE ANALYSIS

New Strategy Cost-Benefit Analysis

Adding Compliance-Related Costs of Using Third Party



Benefits Outweigh Costs

The business's analysis doesn't incorporate the costs of upfront due diligence, ongoing monitoring, and a potential compliance failure.

Costs Outweigh Benefits

After Compliance's cost analysis, the benefits of a prospective third party are no longer justified.

Source: Johnson Controls, Inc.; CEB analysis.

Third-Party Risk Management

Contact us to dive deeper into this report and learn how CEB can help your team implement these strategies to better manage compliance risk while reducing the business cost of third-party use.