Benchmarking third party vendor risk management – global research insights

8th June 2017

Shane McGonigle
Chief Customer Officer
TerraNua DBA MyComplianceOffice
Overview

- Introduction and background
  - Recent decisions by the SEC and SFO
- Results presentation
  - Program maturity levels
  - Decision-makers
  - Budgets
  - Objectives
  - Risks and challenges
- Q&A
- Close

“We believe that great governance is at the heart of great business, helping to protect and promote your reputation”.

Brian Fahey, CEO, MyComplianceOffice
Reputation is valuable

“Lose money and I will forgive you. Lose even a shred of reputation and I will be ruthless. ... Wealth can always be recreated, but reputation takes a lifetime to build and often only a moment to destroy.”

According to a study by the World Economic Forum, on average more than 25 percent of a company's market value is directly attributable to its reputation!

Deloitte 2016 study

MANAGING THIRD PARTY RISK
Incidents on the rise

87% have faced a disruptive incident with third parties in the last 2-3 years
Of which...

28% faced major disruption
11% complete third party failure

DELIVERY MODELS
To insource or outsource TPGM?

58.4% are moving to a centralised in-house function to support third party management
33.6% are unsure about their future direction

REPUTATION ON THE LINE
Third party actions - The threats are real

26.2% have suffered reputational damage
23% have been non-compliant with regulatory requirements
20.6% have experienced breach of sensitive customer data

2016 global survey representing eight major industry segments (over 700 organisational sectors).
Investors also increasingly understand that doing business the right way is an effective path to sustainable and profitable growth. In fact, the publicly traded companies among Ethisphere’s 2017 WMEC outperformed the S&P 500 by 9.6 percent over the last four years—a substantial data point underpinning the link between ethics and performance.

Source: Kroll Anti-bribery & Corruption Benchmarking Report 2017

---

**I INVENTED NOTHING NEW.**
**I SIMPLY ASSEMBLED THE DISCOVERIES OF OTHER MEN BEHIND WHOM WERE CENTURIES OF WORK... PROGRESS HAPPENS WHEN ALL THE FACTORS THAT MAKE FOR IT ARE READY AND THEN IT IS INEVITABLE.**

HENRY FORD
The Development of Third Party Risk Management Practices

Facts are stubborn, but statistics are more pliable.

~ Mark Twain
Introduction

• Emerging area
• People and organizations are finding their feet, some faster than others
• The level of maturity in the management of vendors is variable
• But overall, the Banking Sector reported having more advanced systems
• The reach of regulators is global and getting stronger
• Fines and reputational damage for the business and the individuals is significant
• This report is aimed at helping us all to improve our knowledge by looking at our peers and learning from standards in the category

Sample methodology

• Conducted in October and November 2016 with CefPro, the Centre for Financial Professionals
• 243 respondents globally via questionnaire administered online
• Financial services sector
Regions

Regions where organizations engage with third parties

<table>
<thead>
<tr>
<th>Region</th>
<th>Engagements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia</td>
<td>50.0%</td>
</tr>
<tr>
<td>Latin America</td>
<td>40.0%</td>
</tr>
<tr>
<td>Middle East</td>
<td>30.0%</td>
</tr>
<tr>
<td>Africa</td>
<td>20.0%</td>
</tr>
<tr>
<td>Europe excluding EU countries</td>
<td>10.0%</td>
</tr>
<tr>
<td>Rest of EU</td>
<td>0.0%</td>
</tr>
<tr>
<td>UK</td>
<td>50.0%</td>
</tr>
<tr>
<td>Canada</td>
<td>40.0%</td>
</tr>
<tr>
<td>USA</td>
<td>30.0%</td>
</tr>
</tbody>
</table>

59 different regulators identified

Regulators

Regulators most relevant to your operations

<table>
<thead>
<tr>
<th>Regulator</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other (please list all)</td>
<td>50.0%</td>
</tr>
<tr>
<td>FINRA</td>
<td>40.0%</td>
</tr>
<tr>
<td>OFS</td>
<td>30.0%</td>
</tr>
<tr>
<td>Federal Financial Institutions Examinations Council (FFIEC)</td>
<td>20.0%</td>
</tr>
<tr>
<td>OPSE (Ontario)</td>
<td>10.0%</td>
</tr>
<tr>
<td>FDIC</td>
<td>50.0%</td>
</tr>
<tr>
<td>Securities and Exchange Commission (SEC)</td>
<td>40.0%</td>
</tr>
<tr>
<td>Comptroller of the Currency (COC)</td>
<td>30.0%</td>
</tr>
</tbody>
</table>
This is much more than a US issue

**United Kingdom:** The Prudential Regulation Authority (PRA) has stated that “a firm cannot contract out its regulatory obligations and should take reasonable care to supervise the discharge of outsourced functions.”

**Singapore:** The Monetary Authority of Singapore (MAS) has stated that it “is particularly interested in material outsourcing which, if disrupted, has the potential to significantly impact an institution’s business operations, reputation or profitability and which may have systemic implications.”

**Australia:** The Australian Prudential Regulatory Authority (APRA) aims to ensure that all outsourcing arrangements involving material business activities entered into by a regulated institution are subject to appropriate due diligence, approval, and ongoing monitoring.

**Hong Kong:** The Hong Kong Monetary Authority (HKMA) states that institutions “should not enter into, or continue, any outsourcing arrangements [that] may result in their internal control systems or business conduct being compromised or weakened after the activity has been outsourced.”
Global legislation

- UK Bribery Act and the Modern Anti-Slavery Act
- Brazil’s Clean Companies Act
- Germany’s Act on Combating International Bribery (IntBestG)
- Netherlands (Article 177, 177a and 178 of Dutch Criminal Code). These articles were specifically introduced into the Dutch Criminal Code as a compliance measure of the OECD convention of 1997.
- China’s anti-corruption rules are spread across rules and regulations that include Anti-unfair Competition Law, Provisional Measures on the Prohibition of Commercial Bribery, Criminal Law, and many other judicial decisions and laws.

Maturity

- Goes to the heart of an organizations views and activity with regard to third party risk
  - The importance we attach to third party risk
  - How we allocate resources to deal with the issues
  - The seniority of people we involve in decision-making
  - Relevance to the achievement of our organizational goals
  - Protection and promotion of our corporate finances and reputation
Immaturity leads to problems

Program maturity

1. No policy exists
2. Ad hoc: processes exist but are ad hoc and unpredictable
3. Reactive: processes are reactive and project specific
4. Organized: processes are organized, formalized and documented
5. Controlled: processes are formalized, measured and controlled
6. Mature: processes are highly mature and emphasise system feedback and improvement
Program maturity

Maturity of third party risk management programs

Program maturity

<table>
<thead>
<tr>
<th>How would you currently classify your management of vendor/third party risk management program?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company size</td>
</tr>
<tr>
<td>Under 500 employees</td>
</tr>
<tr>
<td>No policy exists</td>
</tr>
<tr>
<td>Processes exist but are &quot;ad hoc&quot; and unpredictable</td>
</tr>
<tr>
<td>Processes are reactive and project specific</td>
</tr>
<tr>
<td>Processes are organized, formalized, and documented</td>
</tr>
<tr>
<td>Processes are formalized, measured, and controlled</td>
</tr>
<tr>
<td>Processes are highly mature, and emphasize system feedback and improvement</td>
</tr>
</tbody>
</table>
Program maturity

<table>
<thead>
<tr>
<th>How would you currently classify your management of vendor / third party risk management program?</th>
<th>Banking</th>
<th>Other industries</th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy exists</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Processes exist but are 'ad hoc' and unpredictable</td>
<td>6%</td>
<td>17%</td>
</tr>
<tr>
<td>Processes are reactive and project specific</td>
<td>11%</td>
<td>23%</td>
</tr>
<tr>
<td>Processes are organized, formalized and documented</td>
<td>32%</td>
<td>31%</td>
</tr>
<tr>
<td>Processes are formalized, measured and controlled</td>
<td>37%</td>
<td>19%</td>
</tr>
<tr>
<td>Processes are highly mature, and emphasize system feedback and improvement</td>
<td>12%</td>
<td>11%</td>
</tr>
</tbody>
</table>

FCPA Fines 2016

1) 2016 has seen the FCPA hand out a total of 24 corporate settlements totalling $2.6 billion.
2) The largest corporate settlement was in December for $519 million (Teva Pharmaceutical).
3) Four of last years settlements made into the all time top 10 settlements. VimpelCom $397.6mil (9th), Och-Ziff $412mil (6th), Odebrecht/Brasken $419.8mil (5th) and Teva Pharmaceutical $519mil (4th).
4) The average corporate settlement handed out was $108,333,333.
5) There were 8 settlements settled against individuals in 2016.
6) 2016 was the second biggest year for both enforcement actions and settlements since the enactment of the FCPA, only behind 2008 who had the large Siemens settlement for $800mil.
7) The top 3 countries mentioned in settlement cases (since 2014) are Brazil (19), China (17) and Iraq (8).
Deutsche Bank settlement

The Justice Department completed a deal with Deutsche Bank on Tuesday that will require the bank to pay $7.2 billion for its sale of toxic mortgage securities in the run-up to the 2008 financial crisis, the department said.

Deutsche Bank’s United States-listed shares fell 3.2 percent to close at $18.56 on the New York Stock Exchange.

1. Financial and reputational damage is significant

But the damage has been done. After five profit warnings in two years, Rolls-Royce is already fighting against the headwinds of slowing aerospace and energy markets. Now it has to prove that its recovery will be justly earned.

The revelations will undermine the view that the group’s heady growth since privatisation has been mainly based on its engineering excellence. Since 1987 the company’s order book has risen from £2.8bn to £70bn last year. By the end

2. The SFO steps onto the world stage as regulator

“This DPA instantly places the SFO in the big league when it comes to investigating and resolving bribery investigations,” said Barry Vitou, partner at Pinsent Masons. “The amount dwarfs any amount previously contemplated by a UK court in the context of criminal law enforcement.”
Who is responsible?

What department was the primary decision maker within your organization in the decision to develop the third party or vendor risk management program?

Investment levels

Will your budget for third party risk management increase in the next 12 months?

Deloitte believes that the increasing frequency of third party incidents, negatively impacting organisational reputation, earnings and shareholder value, is currently the single-most compelling driver for organisations to invest in TPGRM.
What happens with poor controls?

**Deloitte.**

**Impact of third-party incidents faced by recent survey respondents**

- 26.2% Reputational damage
- 23.0% Financial or transaction reporting errors
- 23.0% Non-compliance with regulatory requirements
- 20.6% Breach of sensitive customer data
- 10.3% Lost business

**Investment levels**

*If you do intend to increase your budget, by what percentage?*

- 0-5%
- 5-10%
- 10-25%
- 25-50%
- More than 50%
Objectives driving the organization

Risk you most want to monitor
“On average 89 third-party vendors access a typical company’s network each week.”

“…only a third (35%) of companies are confident they know the exact number of vendors accessing their IT systems”
Most helpful sources of information

In summary

- Third party risk management is an emerging area
- There is a lot of interest in learning more
- 240+ companies shared their opinions here
- Representing a broad range of financial services companies, large and small
- Banks are the most mature in the programs they are running to mitigate the risks
- The downside risk of financial loss and reputational damage is increasing
- More regulators, more regulation and more enforcement
- Enforcement is becoming a global standard
- Meeting these regulatory requirements is the number one objective
In summary

• Organizations are investing more to do this
• IT/Data Security was identified as the number one area of risk
• There are a multitude of challenges facing firms in managing third parties
• Over 80% of respondents cite inhouse, subject matter experts as one of the most helpful sources of information, followed by professional bodies and trade associations such as the SCCE

Going Forward
Going forward

- You need a robust and operational program
- It must be able to scale and grow with your business
- And with the changes brought on by the evolution of regulation
- Ideally, it will offer one view across all risk and compliance elements in the business
- Realistically, to manage multiple suppliers, multiple transactions, between multiple internal and external parties, the program has to be automated.

44.9% of respondents feel that flexibility and scalability will be the top emerging driver for third party engagement.

55.1% of respondents aspire to have integrated third party risk management systems in a year or more, with 16.5% aspiring to be “best in class”.

Source: Deloitte Study 2016

Comments by enforcement authorities

- “Compliance programs seem strong on paper, but weak in practice”
- “Programs must be industry specific, and metrics oriented”
- “Tone at the top is necessary, but it also must be communicated throughout the organization”
- “Operationalize”
- “Transaction monitoring is essential”
- “Must demonstrate the overall effectiveness of your program”
- “Document, document, document”

Source: Presentation by Keith Darcy, Independent Senior Advisor to Deloitte & Touche LLP
MCO platform

- Affordable SaaS solution
- Scalable into the future
- Integrates with existing systems
- Manage by alerts not reports
- Dashboards deliver improved oversight
- Custom questionnaire builder
- Continuous updates to the software
- Multiple data capture points
- Dedicated implementation team
- Integrated solution
Some helpful sources

- https://www.cefpro.com/
- http://blog.volkovlaw.com/
- https://mco.mycomplianceoffice.com/vendor-risk-management-software
- https://fcpatracker.com/
- http://www.complianceethicsinstitute.org/

Thank You

Download the full research report at
www.mycomplianceoffice.com

Call (866) 951-2279
advance@mycomplianceoffice.com

@mycompliance