# From FCPA to Reputation Risk: The Importance of Applying Internal Controls to the Extended Enterprise

By Matt Kelly

To say that third parties bring risk to a corporation isn’t anything new to compliance officers. Everyone knows that. The phrase itself — “third-party risk” — is so broad that it barely helps when trying to build better compliance programs.

The risks that a third party can bring to a corporation encompass everything from financial risk, to information security risk, to compliance risk. Failure across any of these can result in damaging headlines, enforcement actions, loss of customer trust, and harm to shareholder value. So therefore, the third party also brings reputational risk.

Instead, if corporate compliance professionals want to understand what causes third-party risk and how to reduce it, we need to define the risk that companies face more precisely: ***weak internal controls associated with how you manage your extended enterprise.***

Even if your business has great controls in place for your internal teams and processes, does the same rigor apply to your "extended team" – the "outside" ecosystem that now also supports operations and strategy for so many organizations? And also holds a piece of your reputation in their hands?

This means you need the right controls around:

- how suppliers and vendors enter your third-party ecosystem; and how they are managed and monitored throughout the full lifecycle of the relationship;

- establishing that your third party has the rigorous controls in place that you expect to protect your reputation at both the entity level and the engagement level;

- ensuring that your internal controls extend outside the organization and into how you manage the relationships that make up your extended enterprise.

We've seen numerous examples in the last 12 months where poor internal controls led to problems ranging from anti-bribery failures, to cybersecurity breaches, to reputational damage associated with integrity failures. Businesses have been fined. Senior executives have been fired. Social media campaigns burned long-cultivated corporate reputations to cinders. All of it stemming from poor internal control over third parties.

Companies don't merely need to perform due diligence and ascertain facts about their third parties. They then need to ensure that ***the company acts on those facts accordingly***.

In other words, companies need to impose internal control. They need to bring policy and procedure to bear on specific transactions and third parties – as a part of their extended enterprise. Internal control ***gets something done***.

## Weak Controls in Practice

Recent enforcement actions and media headlines offer several examples of internal control failures. Consider the following:

### Reputation risk

Earlier this year, several companies were hit with news that they had paid exorbitant consulting fees to Michael Cohen, former personal attorney to President Trump. Those fees, far larger than what the companies normally paid to other consultants, ostensibly were for assistance in telecommunications mergers, healthcare policy, and the like. Cohen, a real estate lawyer and owner of taxi medallions, had no such expertise.

***Control considerations:*** Using Cohen in that manner violated several standards of internal control for third parties: Does the company have a clearly articulated reason for using the party? Is the price paid commensurate with the party's skill or services? Can the party deliver the services offered? Those questions are part of guidance for anti-bribery statutes around the world.

The payments to Cohen weren't illegal per se, but the reputation damage was done. The companies involved subsequently ousted the senior executives who approved Cohen and then promised stronger oversight.

### Cybersecurity failures

In September 2018, the Securities and Exchange Commission fined an Iowa broker-dealer firm $1 million for poor cybersecurity procedures. The firm maintained an online portal that contained personal data about its customers. Investment advisers, who worked as independent contractors with the firm, logged into that system remotely to access that customer data.

In 2016 the broker-dealer fell victim to hackers who called the firm's service line pretending to be contractors and then convinced employees to send them password reset emails. The hackers subsequently opened bogus contractor accounts and stole the personal data of 5,600 customers.

***Control considerations:*** According to the SEC order, the firm failed to apply its procedures to the systems used by its independent contractors, who make up the largest part of the firm's workforce.

That scam worked because the firm had not updated its internal controls to prevent identity theft since 2009. For example, the firm did use two-factor authentication for internal employees (say, sending a one-time passcode to an employee's cell phone, before resetting a password); but did not use such authentication for third parties. The firm's internal controls had not been applied to its extended third-party workforce.

## Anti-corruption failures

The SEC and Justice Department also recently hit Petrobras, a Brazilian state-owned oil-and-gas company with a $1.8 billion (yes, billion) penalty for violations of the Foreign Corrupt Practices Act.

The agencies charged that senior company executives worked with Petrobras' largest contractors and suppliers to facilitate bid-rigging and bribery schemes to inflate the cost of infrastructure projects by billions of dollars.

The contractors would pay bribes representing a small percentage of the value of the contracts obtained by Petrobras, which were then split among executives, politicians, political parties and other individuals involved in facilitating the bribe payments.

***Control considerations:*** According to the DOJ, Petrobras executives facilitated the corruption schemes by failing to implement appropriate due diligence procedures for the retention of third-party vendors, "sufficient oversight to prevent the revision of estimates at the conclusion of the bid phase to favor certain bidders," and safeguards to prevent the manipulation of bid participant lists that allowed unqualified bidders into consideration for projects. (1)

There were also significant books-and-records control failures, including false Sarbanes-Oxley 302 sub-certifications. Petrobras admitted that certain executives failed to implement internal financial and accounting controls to continue to facilitate bribe payments to Brazilian politicians and Brazilian political parties.

Two strands of effective compliance (or the lack thereof) weave through all three examples. First, does the company understand the risk this third party truly poses? And second, has the company then implemented sufficient internal controls to reduce that risk to an acceptable level?

*(1) Source: https://www.paulweiss.com/practices/litigation/anti-corruption-fcpa/publications/behind-petrobras-18-billion-fcpa-settlement-an-interesting-accounting?id=27511*

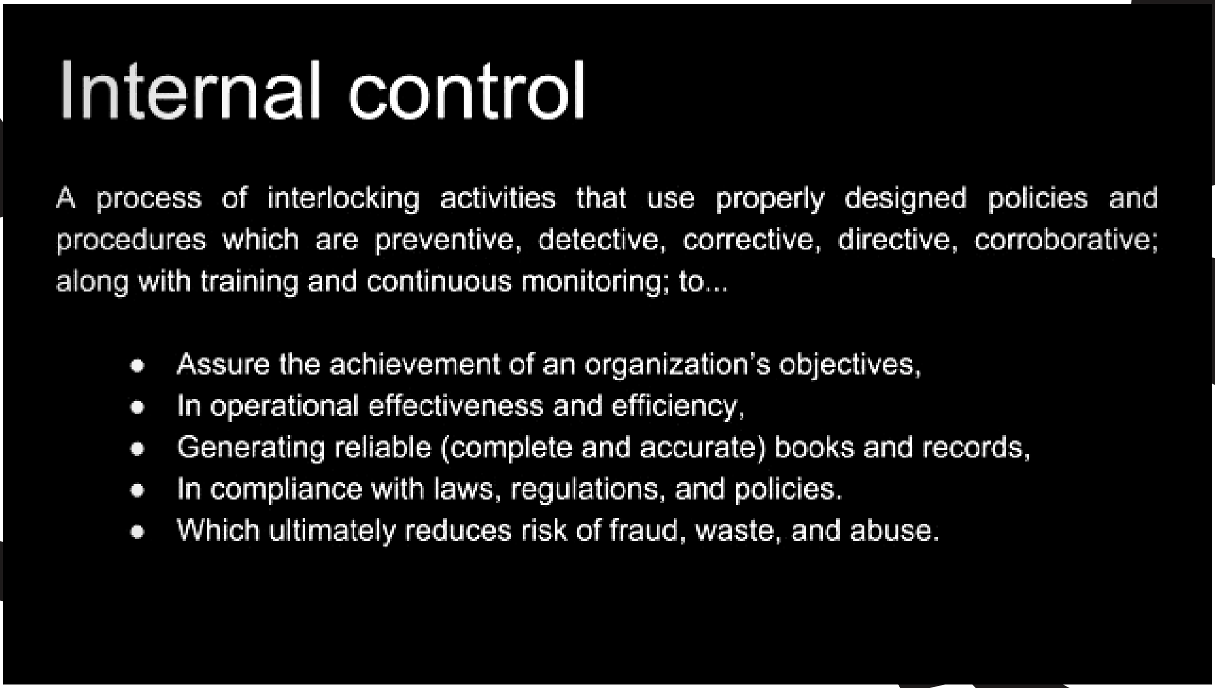
## The Nature of Internal Controls

So what can compliance officers do about weak controls? To start, we should consider the nature of a control — that is, at an abstract level, what a control is supposed to do.

Compliance officers can look to several definitions. Section 13(b)(2)(B) of the Exchange Act lists four items that an effective internal control system should achieve, from transactions happening according to management's authorization; to periodic checks that a recorded asset matches with existing assets. COSO defines a control as a process that provides reasonable assurance the organization can achieve objectives of efficient operations, reliable financial reporting, and compliance with regulations.

Those definitions are useful, but they don't capture the full picture. For example, they don't clearly address threats such as reputation or cybersecurity risk. Questions about materiality and reasonable levels of assurance might be relatively mature for financial reporting, but they are much less clear for risks around corruption, data breach, or reputation harm. Nor do the above definitions say much about what "the process" of a control actually is. Further, they don't account for the extended enterprise – or the ecosystem of vendors and suppliers, that today form such an integral part of a company's strategy, operations and supply chain accountability.

A more useful definition is something like the following. An internal control is —



Internal control

A process of interlocking activities that use properly designed policies and procedures which are preventive, detective, corrective, directive, corroborative; along with training and continuous monitoring; to...

- Assure the achievement of an organization's objectives,
- In operational effectiveness and efficiency,
- Generating reliable (complete and accurate) books and records,
- In compliance with laws, regulations, and policies.
- Which ultimately reduces risk of fraud, waste, and abuse.

Yes, that's a mouthful, but the definition hits on all the right points, and emphasizes the most important one right at the top: An internal control is a process of interlocking activities that use properly designed policies and procedures.

In other words, an effective control has multiple parts that support each other, based upon properly designed policies and procedures.

Properly designed for what? The risk that the organization is trying to manage — including governance of third parties. Hence this definition is flexible enough to address a wide range of risks, including non-financial threats such as cybersecurity or reputation harm. It also compels you to consider all the ways that a control is supposed to work: the preventing, detecting, correcting, directing, and corroborating.

As we said above, a control is action. It puts policy into practice.

## Necessary Components of Control

If that's how effective internal control should function, to prevent the sort of failures we outlined above, then several steps become more important — steps a company must be able to take if it wants to keep third-party risk in check.

**Coordinate risk assessment and policy management**

Risk assessments are crucial in today's fast-changing business landscape, but the implications of any changes in your company's risk profile must be reflected in corporate policies pushed out to employees AND third parties.

That is, the ability to assure that policies and procedures stay current with risk is becoming more important.

That was one failure in companies working with Michael Cohen: they had policies against using questionable third parties overseas, but didn't consider the reputation risk of a questionable domestic third party in today's highly polarized political environment.

It was also the failure in our cybersecurity example above: the firm had strong authentication policies for employees, but didn't extend those policies to its contractors even as the risk of hackers posing as contractors grew painfully clear.

**Articulate the right control environment**

Even under the best of circumstances, today's risks evolve so quickly that policies and procedures can lag behind the threat. So a strong control environment — compliance messages from senior executives, pay structures that reward good conduct, training on ethical values and proper procedure so employees do their jobs without compliance failures, and so forth — becomes critical, since it tries to prepare employees for crises the compliance function hasn't anticipated yet.

We often see weak control environments afoot in FCPA cases, especially in books-and-records cases where employees and third parties manipulate complex sales or bid policies to create the means to bribe. Companies can, and should, impose strong controls to govern these practices — but when people feel pressure to commit misconduct, they usually find a way to do it. Strong, ethical control environments alleviate that pressure.

### Maintain visibility into transactions and beneficial owners

We said above that strong internal control "brings policy and procedure to bear on specific transactions and third parties as they appear in your corporate enterprise." That cannot happen unless your organization can identify when suspicious third parties and transactions do appear in your corporate enterprise.

Identifying suspicious third parties requires due diligence; identifying suspicious transactions requires monitoring. Given the sheer volume of third parties and transactions that today course through even mid-sized enterprises, automated solutions driven by smart use of technology are indispensable.

## Conclusion

The modern business environment involves risks that strike rapidly, and usually strike through third parties the company uses as part of its business operations. Awareness of your third parties is a crucial first step, but it is only the first step. Imposing strong internal controls, suitable for the risks your company has and how third parties might cause a "negative risk outcome," is crucial.

That means connecting risk assessments to policy management, setting a strong control environment, and performing sharper, more accurate due diligence and monitoring. Those are the indispensable traits of a successful compliance program today, and they will only become more important tomorrow.

## About the author

Matt Kelly is a leading compliance industry analyst and consultant, who studies corporate compliance, governance, and risk management issues. He maintains a blog, RadicalCompliance.com, where he shares his thoughts on business issues; and frequently speaks on compliance, governance, and risk topics.
Kelly was named as ‘Rising Star of Corporate Governance’ by Millstein Center for Corporate Governance in the inaugural class of 2008; and named to Ethisphere’s ‘Most Influential in Business Ethics’ list in 2011 and 2013.

Kelly was previously editor of Compliance Week from 2006 through 2015. He lives in Boston, Massachusetts, and can be reached at mkelly@RadicalCompliance.com.

# About Aravo

Aravo Solutions delivers market-leading cloud-based solutions for managing third party governance, risk, compliance, and performance. We help companies protect their business value and reputation by managing the risks associated with third parties and suppliers, and to build business value by ensuring that their third party relationships are optimized.

Since 2000, leading global brands across a diverse range of industries have counted on Aravo for their end-to-end enterprise supplier and third party risk management. Aravo has also distilled this experience and best-in-class technology into rapid time-to-value applications that help companies manage a wide range of programs including: anti-bribery and anti-corruption, responsible sourcing, data privacy, information security, GDPR, financial services regulatory compliance and know your third party programs.

Providing unrivaled regulatory agility and ease-of-use, together with actionable executive reporting, Aravo supports a user base of 136,000 corporate users, managing more than 4.5 million third party users in 36 languages and 154 countries. Aravo is headquartered in San Francisco, with offices and partners across the US, Europe, and Asia.

Aravo was recognized as a leader by independent analyst research firm Forrester Research Inc., in The Forrester Wave™: Supplier Risk And Performance Management Platforms, Q1 2018. Aravo is the top-ranked vendor in the current offering category.

Aravo has been recognized with GRC 20/20's Value Award for Third Party Management for providing measurable value in GRC efficiency, effectiveness and agility, and with the GRC 20/20 Innovation Award for Aravo for GDPR. Aravo was named as a Category Leader with the highest "Completeness of Offering" of any provider in the Chartis RiskTech Quadrant® for Third Party Risk Management Solutions 2017, was named a Challenger in the 2017 Gartner® Magic Quadrant for IT Vendor Risk Management.