Vendor Risk Management:
Three Steps for the Capabilities You Need

Matt Kelly
Radical Compliance
mkelly@RadicalCompliance.com

Edwin Broecker
Quarles & Brady
Ed.Broecker@quarles.com

Fernanda Beraldi
Cummins Inc.
fernanda.beraldi@cummins.com

Who are these people?

Matt Kelly, editor
Radical Compliance

Ed Broecker, partner
Quarles & Brady

Fernanda Beraldi
Cummins Inc.

Agenda

- Due diligence: what the law requires you to look for, how to find it, what to do with it when you find it
- Risk assessments: assessing multiple types of risk in one versatile assessment process
- Put it into practice: how Cummins manages vendor risk across one whole planet
- Q&A

Part I:

Due diligence & finding beneficial owners

Edwin Broecker
Quarles & Brady LLP

Introduction

A. Supply chains continue to be more global and complex
B. Consumers demanding more ethical behavior throughout entire supply chain
C. Many large corporations have tens of thousands of suppliers. According to a recent Forbes article, Procter & Gamble had more than 75,000 suppliers, Walmart more than 100,000 suppliers

Connectography, Khanna, P. 2016
https://worldview.stratfor.com/article/connecting-world-through-infrastructure

Quarles & Brady LLP

Third Parties Create Risk

2012 FCPA Guidance from Justice Department and SEC:

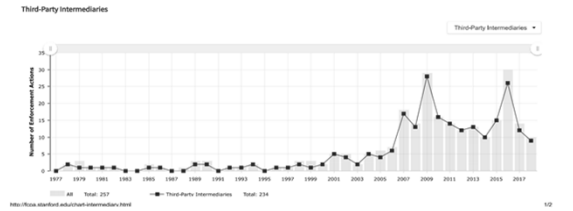
DOJ and SEC FCPA enforcement actions demonstrate that **third parties, including agents, consultants, and distributors, are commonly used to conceal payment of bribes to foreign officials in international business transactions**.

Risk-based due diligence is particularly important with third parties and will also be considered by DOJ and SEC in assessing effectiveness of a company's compliance program.

Quarles & Brady LLP

FCPA Third Party Enforcement

91 percent of all FCPA enforcement actions involve third parties



Foreign Corrupt Practices Act Clearinghouse (Stanford Law School).

Quarles & Brady LLP

Third-party liability

A. Significant risk

B. Liability for third-party actions

C. Payment doesn't have to be for a cash bribe

D. No actual knowledge of corrupt payment required
   1. Aware of high probability of corruption
   2. Willful blindness

E. Requires due diligence into third parties
   1. Red Flags

Quarles & Brady LLP

FCPA Elements

A. Anti-Bribery: FCPA anti-bribery provisions make it illegal to:
   - **a) Corruptly** offer or provide;
   - **b) Money or anything of value;**
   - c) to **officials of foreign governments**, foreign political parties, or public international organizations;
   - d) with **intent to obtain or retain business**.

B. Books & Records
- Issuers must make and keep accurate books, records, and accounts that, in reasonable detail, accurately and fairly reflect the issuer's transactions and disposition of assets.

A. Internal Controls
- Issuers must devise and maintain reasonable internal accounting controls aimed at preventing and detecting FCPA violations

Quarles & Brady LLP

Not Just FCPA

A. Export Control Issues

- Licenses depend on an item's technical characteristics, the destination, **the end-user,** and the end use

A. Trade Sanctions

- OFAC maintains comprehensive list of Specially Designated Nationals (SDNs)
- All commerce with such individuals prohibited

Quarles & Brady LLP

Export Controls Risks - issues

A. Need for license

B. Increased enforcement
- Debarment
- Reputational risks
- Big fines

A. Successor liability

B. International inconsistency for sanctions
- Iran
- Cuba

Quarles & Brady LLP

Export Controls Risks - keys

A. Best Practice: **Know your customer/agent/distributor/supplier**

B. BIS maintains a list of warnings that may indicate problems
- https://www.bis.doc.gov/index.php/enforcement/oee/compliance/23-compliance-a-training/51-red-flag-indicators

A. Train employees on risks of diversion

B. Unusual transactions

Quarles & Brady LLP

DOJ/SEC Resource Guide - 2012

Some Elements of Effective Compliance Program

1. As part of **risk-based due diligence**, companies should understand qualifications and associations of its third-party partners, including its business reputation; and any relationships with foreign officials.
2. Companies should understand business **rationale for including the third party** in transaction.
3. Companies should undertake some form of **ongoing monitoring** of third-party relationships.
   a) update due diligence periodically;
   b) exercise audit rights;
   c) provide periodic training;
   d) annual compliance certifications from third party.

Quarles & Brady LLP

DOJ Guidance

A. February 2017 DOJ published 'Evaluation of Corporate Compliance Programs'

B. Section 10. Third-Party Management

- **Risk-Based and Integrated Processes**. How has the company's third-party management process corresponded to the nature and level of the enterprise risk identified by the company? How has this process been integrated into the relevant procurement and vendor management processes?
- **Appropriate Controls.** What was the business rationale for the use of the third parties in question? What mechanisms have existed to ensure that the contract terms specifically described the services to be performed, that the payment terms are appropriate, that the described contractual work is performed, and that compensation is commensurate with the services rendered?
- **Management of Relationships.** How has the company considered and analyzed the third party's incentive model against compliance risks? How has the company monitored the third parties in question? How has the company trained the relationship managers about what the compliance risks are and how to manage them? How has the company incentivized compliance and ethical behavior by third parties?
- **Real Actions and Consequences**. Were red flags identified from the due diligence of the third parties involved in the misconduct and how were they resolved? Has a similar third party been suspended, terminated, or audited as a result of compliance issues? How has the company monitored these actions (e.g., ensuring the vendor is not used again in case of termination)?

Quarles & Brady LLP

OECD - Good Practice Guidance

A. Not just in the United States

B. OECD (Organization for Economic Cooperation and Development) published Guidance

C. Companies should consider, inter alia, the following good practices for ensuring effective internal controls, ethics, and compliance programmes or measures for the purpose of preventing and detecting foreign bribery:

Section 6. ethics and compliance programmes or measures designed to prevent and detect foreign bribery applicable, where appropriate and subject to contractual arrangements, to third parties such as agents and other intermediaries, consultants, representatives, distributors, contractors and suppliers, consortia, and joint venture partners (hereinafter "business partners"), including, inter alia, the following essential elements: i) properly documented risk-based due diligence pertaining to the hiring, as well as the appropriate and regular oversight of business partners; ii) informing business partners of the company's commitment to abiding by laws on the prohibitions against foreign bribery, and of the company's ethics and compliance programme or measures for preventing and detecting such bribery; and iii) seeking a reciprocal commitment from business partners.

Good Practice Guidance on Internal Controls, Ethics, and Compliance Adopted 18 February 2010

Quarles & Brady LLP

ISO 37001

2016 ISO Anti-Bribery Standard

Recommends **due diligence procedures implemented by the organisation on its business associates should be consistent across similar bribery risk levels,** so business associates in locations or markets with a higher risk of bribery would need a significantly higher level of due diligence than those in low bribery risk locations or markets.

- Due diligence should be commensurate with risk
- Monitor the Red Flags
- Watch Lists are not sufficient
- Direct and indirect shareholders and top management need to be checked

Quarles & Brady LLP

Best Practices

A. Conduct Risk Assessment
1. Review where and how business is conducted and implications for where corruption may creep in

B. Draft/Revise Policies and Procedures
1. Policies and procedures should be tailored to organization
2. Policies should be based on the results of the risk assessment

C. Develop appropriate program governance
1. Communication
   a) "Tone at the top"
   b) "Mood in the middle"
   c) "Buzz at the bottom"
2. Independence and reporting to board

D. Publicize, Alert and Train Employees, Agents and Contractors
1. Initial and ongoing effective training
2. Live or virtual
3. Maintain record

E. Audit, Monitor and Report
1. Ensures that issues are reported
2. "Trust but verify"

F. Enforcement
1. Consistent and appropriate

Risk Assessment
Policies
Organizational structure & governance
Train
Audit and Monitor
Enforce
Plan and Improve

Quarles & Brady LLP

Part II:

Risk assessments

Matt Kelly
Radical Compliance

Remember what a risk assessment does

1. Identify the hazards
2. Decide who might be harmed, and how
3. Evaluate the risks, decide on control measures
4. Record findings and implement them
5. Review assessment and update as necessary

— Royal Society for the Prevention of Accidents

Bad news: the many hazards vendors pose

1. Corruption
2. Money-laundering
3. Cybersecurity
4. Human trafficking
5. Fraud
6. Supply chain & operations disruption

Versatile risk assessments — sounds great!

- Easy concept to grasp: add more fields to your assessment questionnaire
- Sometimes easy to do, because the risks are similar
- 'Does your company…'
  - Employ low-skilled foreign or migrant workers directly or via recruiters?
  - Allow migrant workers to cancel their contracts with no financial penalty?
  - Check proof-of-age and work eligibility documents for adherence to law and company policy?
  - Employ sub-agents or other intermediaries that might do business on your behalf?
  - Allow migrant workers to cancel their contracts with no financial penalty?
  - Check permitting and ownership documents for adherence to law and company policy?

Plenty of risk assessment raw material

Cybersecurity
- NIST standards
- AICPA trust principles
- Any Big 4 firm

Anti-Corruption
- Transparency Int'l
- Gov't agencies
- Any Big 4 firm
- Any GRC vendor

Human Trafficking
- Social Responsibility Alliance
- Human Trafficking Hotline
- Any Big 4 firm

Ethical Sourcing
- Social Responsibility Alliance
- Other companies
- Any Big 4 firm
- Lots of GRC vendors

Challenge No. 1: Setting correct scope

- What are the business objectives?
- What are the regulatory requirements?
- How does your business process **actually** work?

Ex: cybersecurity assessments based on AICPA 5 Trust Principles

- Assess all five, and you may be over-compliant;
- Assess wrong ones, and you're under-compliant

Hardest part: *defining the specific inclusions and exclusions*

Challenge No. 2: Building correct process

- Remember the perils of getting certifications
  - Vendors lie
  - Employees get confused
  - Messages get mixed, signals get crossed
- Steal ideas from SOX compliance processes on web-based processes
- Study what can be automated, what shouldn't be automated
  - And *which mix of automation and human checks works for you*

Part III:

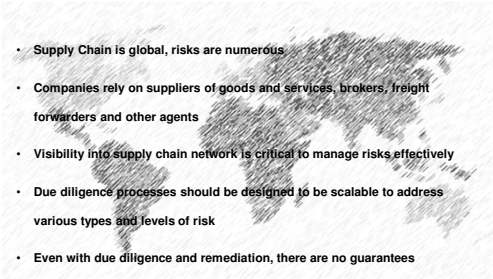
How Cummins Inc. manages risk

Fernanda Beraldi
Cummins Inc.

Cummins Global Presence

60,000 employees
190+ countries and territories
Operations on 6 continents
700 distributor locations
7,000 dealer locations
$20 Billion in revenues (2017)
4,000 direct vendors
19,000 indirect vendors

Global Risks



- **Supply Chain is global, risks are numerous**
- **Companies rely on suppliers of goods and services, brokers, freight forwarders and other agents**
- **Visibility into supply chain network is critical to manage risks effectively**
- **Due diligence processes should be designed to be scalable to address various types and levels of risk**
- **Even with due diligence and remediation, there are no guarantees**

Best Practices

- Due Diligence, Monitoring, Audits
- Contract Provisions
- Training Programs

28

Best Practices

Adequate Internal Controls for Vendor Risk Include:

- Maintenance of fair and accurate books, records and accounts
- A compliance code, standards and procedures designed to detect and deter violations
- Risk-based due diligence on vendors
- Exercise of reasonable oversight and monitoring
- Documentation of relationships, with standard contractual provisions to prevent violations and enable audit, termination, other remedies

29

Best Practices

Know Your Partner

Understand the purpose of your due diligence

- Identify the risks most relevant to you (legal compliance plus other business risk)
- Establish a third-party risk profile, which may vary by geographic location or project

Risk considerations:

- Understand beneficial ownership, government relationships, sanctioned individuals
- Identify your concerns – they won't be the same for each partner:
  - bribery and corruption, fair competition, human rights sensitivities, environmental crimes
- Determine financial viability of prospective business associate
- Identify parties presenting **material** risks

Goal: Develop reasonable, objective basis to proceed (or not) with prospective business associate

30

Best Practices

Due Diligence in Practice

- Assign responsibility for due diligence activity, with independence, checks and balances
- Procurement along with business line – with ultimate decision in contracting – is responsible for due diligence
- Support from Legal Department and/or Compliance personnel
- Clearly defined process

Tools

- Global lists, RPS tools, questionnaires, third-party due diligence, Google
- Ongoing monitoring

Increase due diligence based on risk levels, for example:

- Level I – screening against global watch lists; denied party lists etc.; Business credit report; D&B etc.; Publicly available info on business
- Level II – In-country Records and database searches; Individual background checks on principals and key employees; Questionnaires; Telephone or in-person interviews; Reference checks and queries to industry; Financial records
- Level III– Interviews of personnel; On-site visits and inspections; In-country investigation; In depth background checks; Independent audits; Reference checks and queries to industry; Financial records

31

Identify the Red Flags

- Country's reputation for corruption
- Credible negative rumors or media reports regarding vendor; or vendor history of investigations, indictments, convictions for criminal activity
- Customer or government employee recommends, requests, insists that company work with specific vendor
- Vendor has financial, family, or other close personal ties to government employees
- Vendor's employees recently were government employees
- Vendor is owned by a current government employee, or employs current government employees

32

Identify the Red Flags (cont.)

- Unusual payment methods, other odd requests
- Requests for cash payments, payments to numbered accounts, or bearer instrument
- Requests for payment in third country or to entity not party to the contract
- Requests for extraordinary or last-minute expenses not anticipated by contract
- Vendor says it needs more money with vague explanations: to "clear your items/facility," "fix our problems," "take care of our friends," "make necessary arrangements" or because "you know how things are here"
- False or misleading invoices or other documentation, including invoices for "services rendered" or "services fees" without documentation on services provided or purpose of fees

33

Identify the Red Flags (cont.)

- Requests for unusually high commissions or fees
- Vendor regularly makes facilitating or expediting payments
- Vendor makes political donations or charitable contributions that could be attributed to the company
- Provision of travel or entertainment to serving government employees (including military and police officers of all grades)
- Lack of significant experience, proper qualifications, or appropriate facilities or staffing to perform the required services
- Excessive entertainment expenses generally
- Extensive use of petty cash

34

Identify the Red Flags (cont.)

- Vendor is experiencing financial difficulties
- Use of agents
- Refusal to disclose owners, principals, 'silent partners,' or otherwise provide requested information
- Use of shell or holding companies or blind trusts, especially structures that are nested or involve multiple jurisdictions
- Objections to acknowledge company policies
- Refusal to certify compliance with anti-corruption laws and policies
- Failure to document expenses properly

35

When you find a red flag…

Do Not Ignore It

- Further more in-depth review
- Invoke contractual provisions
- Comfort letter
- Exclude as supplier

Investigate

If necessary, exclude; or include with safeguards to prevent illegal or unethical activity

- Contractual provisions requiring compliance
- Audit rights
- Contractor due diligence on subcontractors
- Require contractor to flow-down compliance to subcontractors

36

Best Practices: Contract Provisions

- Partner with the legal function
- Consider drafting assumptions; U.S. v. local law
- Enforceability
- Covenants
- Reps and warranties
- Audit rights
- Indemnification; payment suspension; termination rights

37

Best Practices: Training Programs

- Train and retrain employees on due diligence, monitoring for red flags
- Provide training to vendors – which ones?
- Is it worth training all the vendors on the same topic?
- Understand and address cultural considerations
- Attitude, importance to written contracts

38