Visibility Into Third Parties

Web Hull

Iron Mountain

Sr. Privacy & Compliance Specialist

Visibility Into Third Parties

Lots of Areas to Monitor & Audit

- ✓ Privacy, Data Protection, & Security
- ✓ Anti-Corruption & Anti-Bribery
- ✓ OFAC
- ✓ Export Controls
- ✓ Anti-Money Laundering
- ✓ …

Visibility Into Third Parties

Why Monitor & Audit?

- ✓ Commitment to your customers
- ✓ Required by Law, Regulation, Regulators, Standards, Contract, …
- ✓ Mitigate Potential Damages – Effective Compliance Program
- ✓ Risk Management

Visibility Into Third Parties

What Do You Want to Know About Your Third Parties?

- ✓ Do they have the right controls & processes in place
- ✓ Are they executing these controls & processes effectively
- ✓ Do they have an effective program to prevent & detect …

Visibility Into Third Parties

It Starts Early & It Starts Inside

- ✓ Selecting Third Parties
  - ➢ Risk Ranking – High, Medium, Low
  - ➢ Initial Assessment of Controls
  - ➢ What's in the Contract – Audit Rights, Standards, Corrective Action, Termination, …

Visibility Into Third Parties

Determining Who & When to Monitor and Audit

- ✓ Periodic Focused Risk Assessment
  - ➢ By Outsourced Function
  - ➢ Change in business relationship
  - ➢ What's in the news
  - ➢ Frequency vs. Risk

Visibility Into Third Parties

How to Monitor & Audit- Reach Out & Evaluate!

- ✓ Learn from your customers – (Free)
- ✓ Third-party Attestations & Certifications – SOC, PCI, NAID, ISO, … - (Free & Easy)

Visibility Into Third Parties

How to Monitor & Audit – Reach Out & Evaluate!

- ✓ Self Certifications – Safe Harbor, Your Own Form, … (Free & And a little work)
- ✓ Questionnaire (Not Free & Requires Work)
- ✓ On-site Audit (Expensive & Hard Work)

Visibility Into Third Parties

Questions & Choices

- ✓ Who is going to do this job – Inside Staff, Third Party, Hybrid?
- ✓ What's the cost & who is going to pay – Centralized, Business Unit, Allocated, …?

Visibility Into Third Parties

Questions & Choices

- ✓ How do I analyze the responses?
- ✓ How do I follow-up on findings?
- ✓ What am I going to do with all this documentation?

Visibility Into Third Parties

Maturity of Monitoring & Auditing

1. Privacy, Data Protection, & Security – Quite Mature
2. Anti-Corruption & Anti-Bribery – Getting There
3. Other – Early Going

NAVEX GLOBAL™
The Ethics and Compliance Experts

Getting Better Visibility Into Third Parties

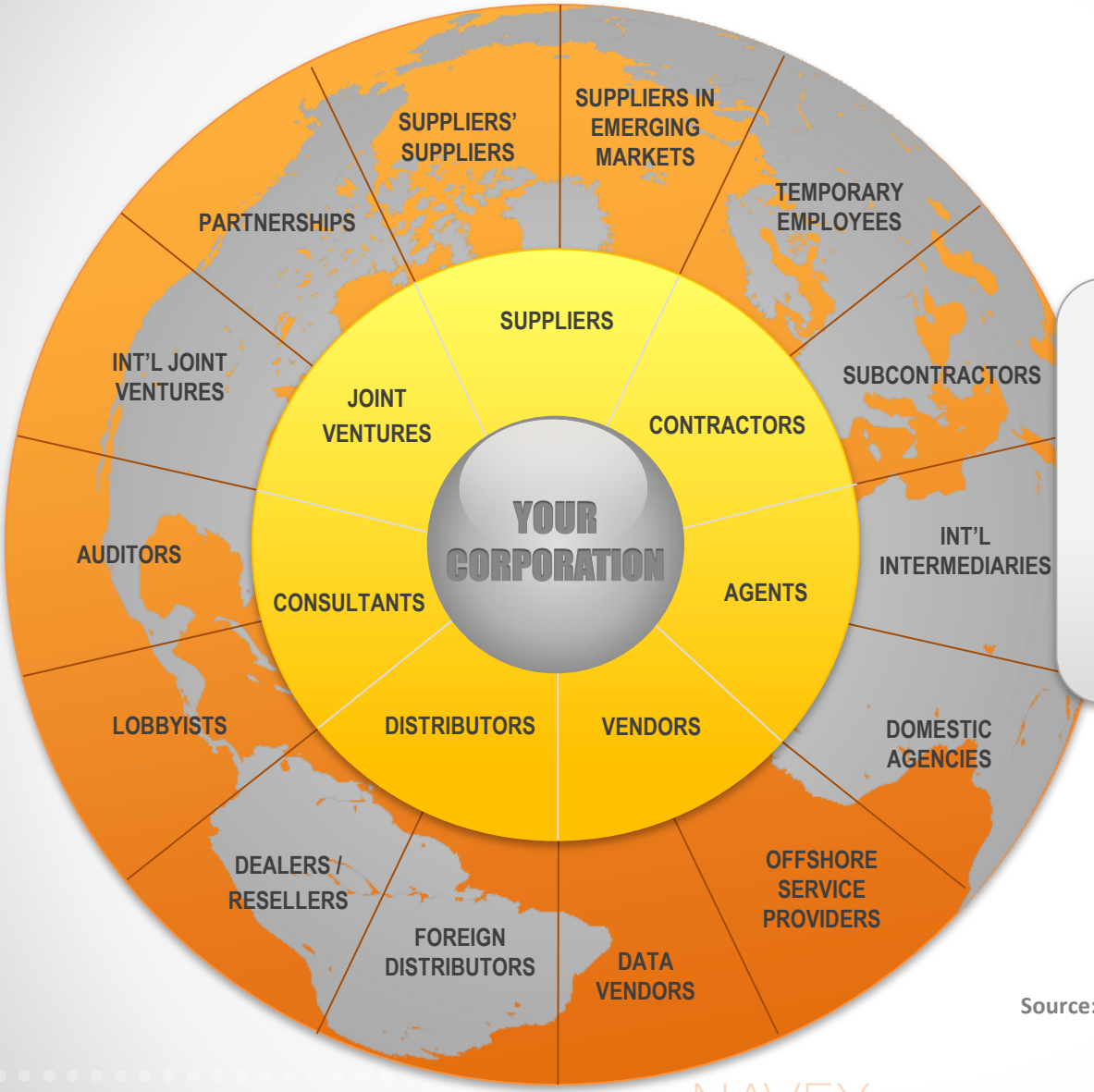
Bob Conlin, NAVEX Global & Web Hull, Iron Mountain

NAVEX Global Ethics & Compliance Solutions

NAVEX Global supports the ethics & compliance programs of more than 8,000 organizations worldwide:

- Hotline
- Case Management
- Policy Management
- On-line Training
- Advisory Services
- Advance Analytics
- Awareness Programs
- **Third Party Risk Management**

Third Party Risk: A Complex Network of Relationships



A High Level of Complexity

Corporations need to manage divergent legal relationships across a multitude of partners, and struggle to gain visibility into often-hidden risks.

Source: Compliance and Ethics Leadership Council

Why Manage Third Party Risk?

Among Ralph Lauren Corporation's remedial measures have been new compliance training… and strengthening its internal controls and its procedures for third party due diligence.

Worldwide third-party relationships under scrutiny.

UK Bribery Act

Individuals risk up to ten years in prison with substantial fines. Organizations risk unlimited fines, debarment from EU contracts, and the confiscation of the value of corruptly obtained contracts.

US Dept of Justice

Encourages companies to "exercise due diligence and to take all necessary precautions to ensure that they have formed a business relationship with reputable and qualified partners and representatives."

What will investigators focus on?

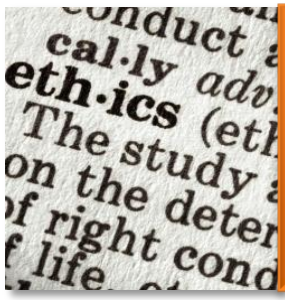
- Are you acting in good faith?
- Do you have a healthy, robust compliance program?
- What is the likelihood of the offense reoccurring?
- Did your compliance program uncover this issue?
- How did you respond?
- If this issue identified weaknesses in your compliance program, have they been corrected?

Types of Potential Third Party Risk

IDENTITY

CONFLICTS

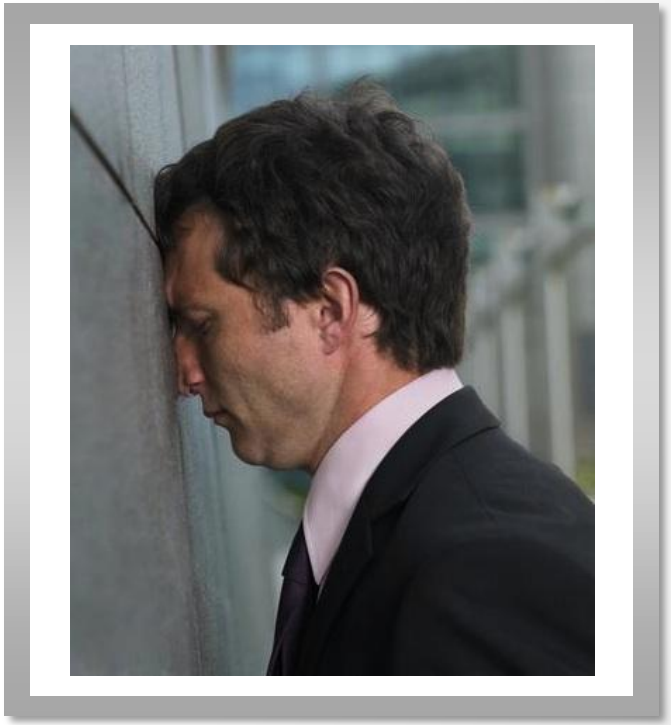
REPUTATION



COMPLIANCE

Why is Third Party Management So Hard?

- Evolving regulatory landscape
- No one clear owner in company
- High stakes for failure
- Resistance by business & partners
- Inefficient and manual processes
- Growth in emerging markets



Best Practice Approach to Third Party Risk Management

What we heard gathering requirements:

- Get us out of email!
- Put the questionnaire online
- Put everything in one place
- Bring down the cost of reports; Different levels of reports based on risk
- Multiple data sources
- Fast turnaround; Help us chase slow responders
- Easy to deploy across business units and geographies
- Easy for third parties and internal business partners to adopt

Risk Adjusted Approach to Third Party Management

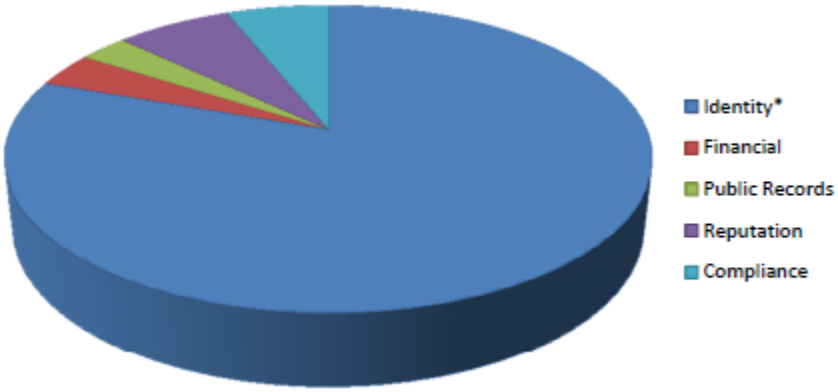
- Moves process online
- Automates routine tasks
- Enables central control & local application
- Manages relationships
- Configures for easy and flexible deployment

NAVEX GLOBAL™
The Ethics and Compliance Experts

DASHBOARD

Overall Risk Assessment

Risk Distribution



Summary - Effective Third-Party Risk Program

- Conduct due diligence before you enter into new relationships
- Assess risk associated with existing third party network
- Apply appropriate due diligence based on risk assessment
- Create a phased project plan to identify, prioritize, and address greatest risks first
- Audit, score, remediate and monitor
- Share training & policies
- Automate for effective, efficient management