What Compliance & Risk Professionals Should Know About 3rd-Party Risk and New DOJ Guidance

Michael Rasmussen, GRC Analyst and Pundit | GRC 20/20 Research, Inc.
Sam Abadir, Director of Industry Solutions | NAVEX Global

What Compliance & Risk Professionals Should Know About 3rd-Party Risk and New DOJ Guidance

About our Guest Presenter

Michael Rasmussen

GRC Analyst and Pundit, GRC 20/20 Research, Inc.

Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC). With 27+ years of experience, Michael helps organizations improve GRC processes and choose technologies that are effective, efficient, and agile. He is a sought-after keynote speaker, author, and advisor and is noted as the “Father of GRC” — being the first to define and model the GRC market in 2002 while at Forrester.

About our Presenter

Sam Abadir

Director of Industry Solutions, NAVEX Global

Sam Abadir has more than 20 years of experience helping companies realize value through improving processes, identifying performance metrics, and understanding risk. Sam is a veteran of both the Big 4 Consulting world and the Software Development industry with over 20 years of experience managing teams from two to 400 people. He is currently working to educate the world on governance, risk and compliance, and help organizations use the data and content around them to better manage risk.

- Top GRC Challenges
- Increased Scrutiny
- Increased Scrutiny from the DOJ
- Managing the Third-Party Lifecycle

1

Top GRC Challenges

Top Challenges of Managing 3rd-party GRC Today

The environment is getting more complex and interdependent

1. It is not just managing risk; it is also governing relationships
2. Brick-and-mortar business is a thing of the past
3. Today's organization is a web of third-party relationships and transactions
4. Insiders include not just employees, but also third parties

2

Increased Scrutiny

Increased Scrutiny from Regulators

The COVID pandemic environment makes compliance harder, but enforcement isn't going away

- Greater scrutiny is upon us
- Regulations, lawsuits, enforcement actions
- FCPA, UK Bribery Act, UK Modern Slavery Act, Sapin II, Conflict Minerals, CCPA, GDPR – It's acronym soup of regulation that impacts 3rd party relationships

3

Increased Scrutiny: From the DOJ

Updated 2020 Guidance for Corporate Compliance Programs from the Department of Justice

The word "third party" *is mentioned 33 times*

in the DOJ's new guidance found in the Evaluation of Corporate Compliance Programs.

4

Managing the Third-party Lifecycle

Managing the Third-party Lifecycle

Initial due diligence is not sufficient

- Onboarding and initial due diligence
- Ongoing monitoring and due diligence throughout relationship
  - This should happen periodically
  - Triggered by events or metrics
- Continuous improvement, periodic testing, and review
  - Leveraging controls for control testing
  - Managing control effectiveness
- Managing and resolving issues
- Offboarding

Q&A

Thank You!