NAVEX GLOBAL

How to Manage the Future Impacts of Covid-19 on Third Party Risk and Compliance

Sam Abadir, CISM
Director, Industry Solutions – NAVEX Global

0

Agenda

- Third Party Risk and Compliance Impacts
- Third-Party Risk Framework
- Ongoing Monitoring & Effective Interpretation
- Approach

NAVEX GLOBAL

1

Third Party Risk and Compliance Impacts

NAVEX GLOBAL

2

What Are Third Parties?

- Your organization does not stand alone

Your Organization

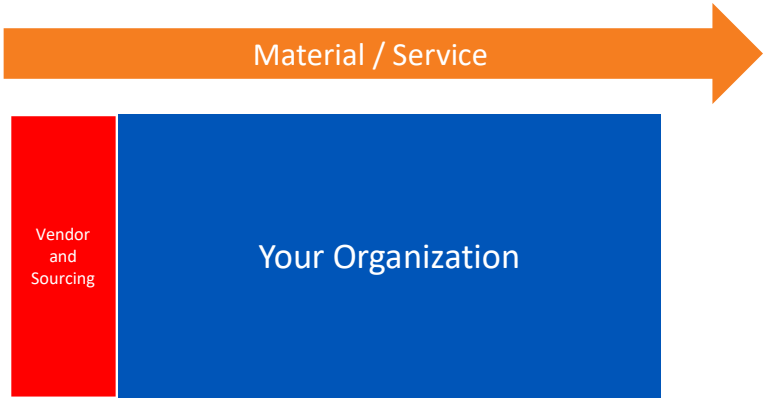
NAVEX GLOBAL

3

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

What Are Third Parties?

- Your organization does not stand alone
- You depend on suppliers, consultants, trade partners, and other third parties to deliver your materials or services

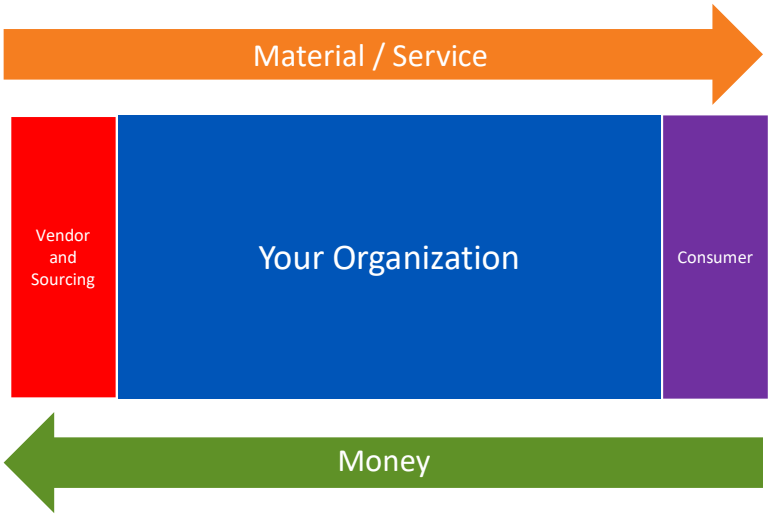


NAVEX GLOBAL

4

What Are Third Parties?

- Your organization does not stand alone
- You depend on suppliers, consultants, trade partners, and other third parties to deliver your materials or services
- Don't forget – Customers are also third parties that supply you with money



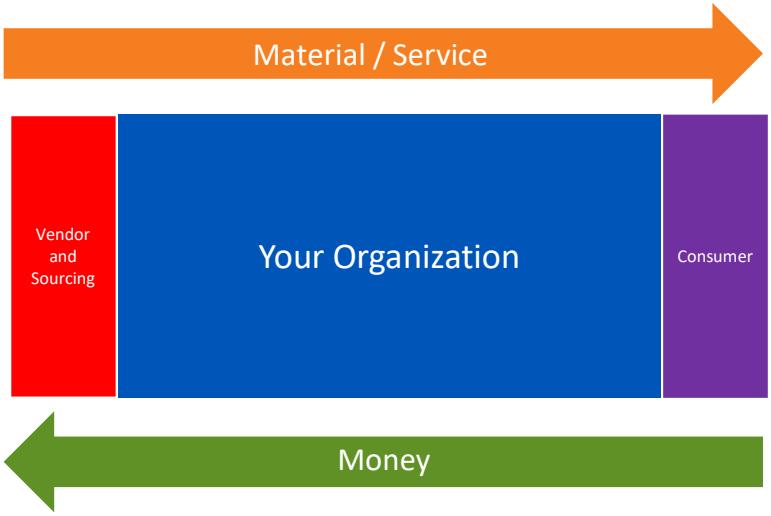
NAVEX GLOBAL

5

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

What Are Third Parties?

- Your organization does not stand alone
- You depend on suppliers, consultants, trade partners, and other third parties to deliver your materials or services
- Don't forget – Customers are also third parties that supply you with money
- Because of critical failures from all types of third parties there is an ever expanding regulatory and compliance focus on managing third party risk



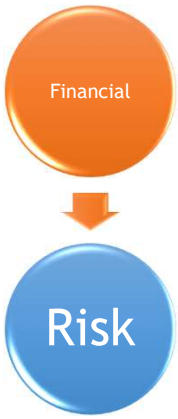
NAVEX GLOBAL

6

Third Parties Bring Risk To Your Organization

Financial

- Are your vendors financially able to support operations that impact you?
- Are you able to financially support operations for your vendors? Will they support you in a time of need?



NAVEX GLOBAL

7

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Third Parties Bring Risk to Your Organization

Operational

- Today's global pandemic is bringing third party operational risk to the forefront
- Can your suppliers fulfill their obligations on time and at the quality level contracted for?
- Do your customer's operations and supplier base impact their need for your product and service?

NAVEX GLOBAL

8

Third Parties Bring Risk to Your Organization

Reputational

- Are your third parties following their compliance obligations?
- The goodwill you build can be ruined by third parties seemingly out of your control

NAVEX GLOBAL

9

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Third Parties Bring Risk to Your Organization

Regulatory

- Failure by your third parties to follow the law often impacts your organization
- Insider trading should be a heightened concern with current market conditions

NAVEX GLOBAL

10

Third Parties Bring Risk to Your Organization

Compliance

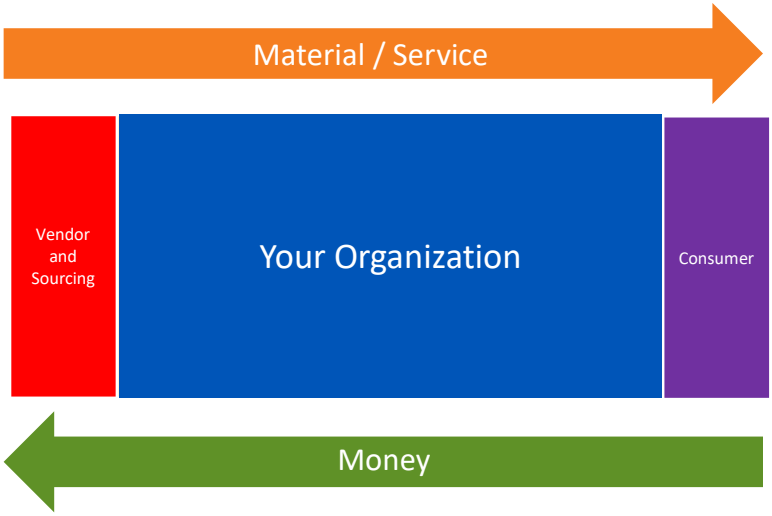
- Bribery, corruption, privacy, fraud, ethical conduct, cybersecurity all have compliance impacts
- Compliance with quality and security standards at higher risk with work from home

NAVEX GLOBAL

11

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Third Parties

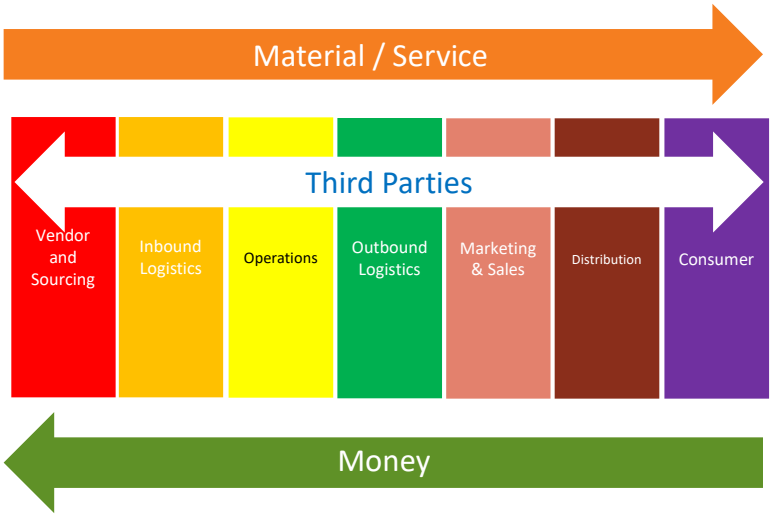


NAVEX GLOBAL

12

Third Parties

- Third parties put your organization at risk – and that risk can ripple throughout the business



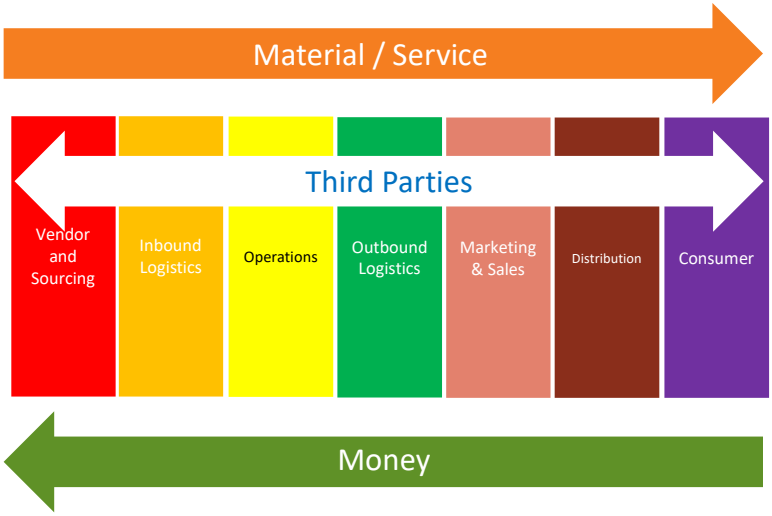
NAVEX GLOBAL

13

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Third Parties

- Third parties put your organization at risk – and that risk can ripple throughout the business
- Many standards and regulations explicitly call for the management of third party risk

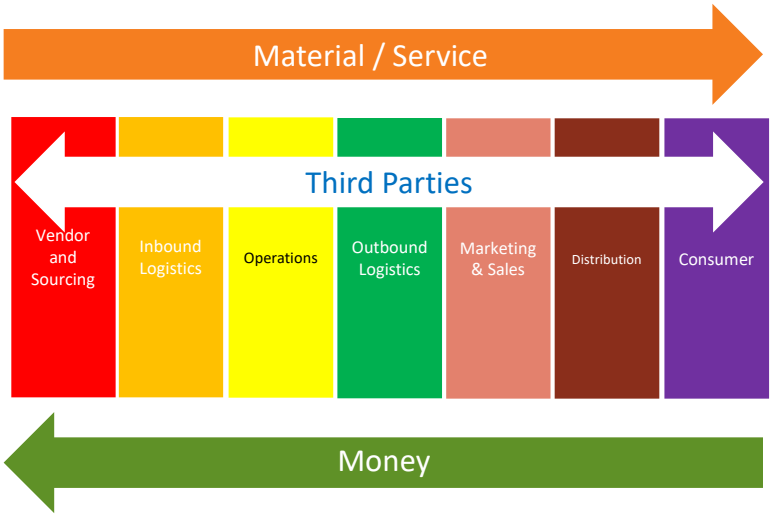


NAVEX GLOBAL

14

Third Parties

- Third parties put your organization at risk – and that risk can ripple throughout the business
- Many standards and regulations explicitly call for the management of third party risk
- As compliance leaders you must take an active interest or manage that risk to achieve your goals



NAVEX GLOBAL

15

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

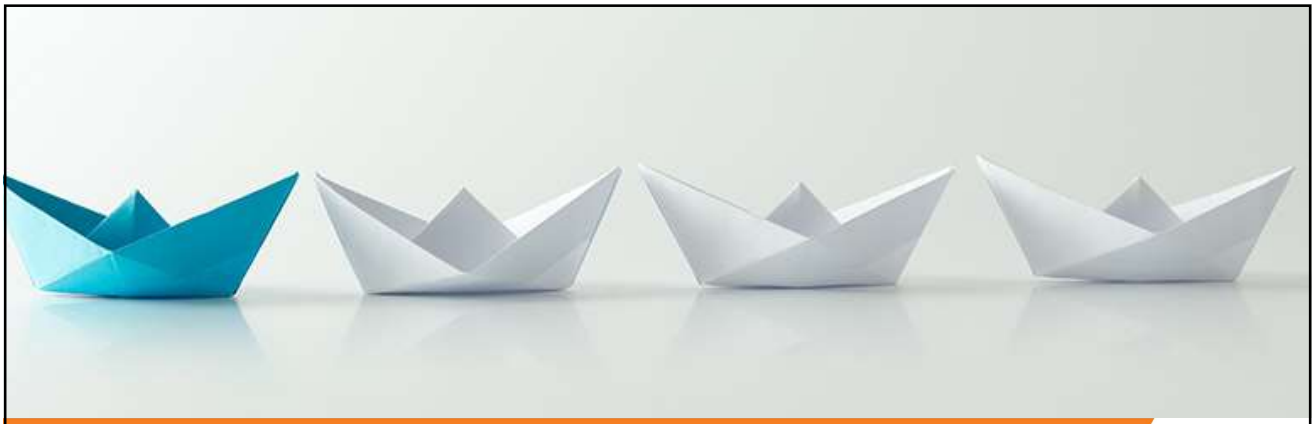
Poll Question

Which of these attributes of third-party risk are you most concerned about?

- Financial
- Operational
- Reputational
- Regulatory
- Compliance

NAVEX GLOBAL

16



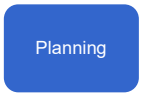
Third-Party Risk Framework

NAVEX GLOBAL

17

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Designing an Effective Vendor Risk Process



Planning

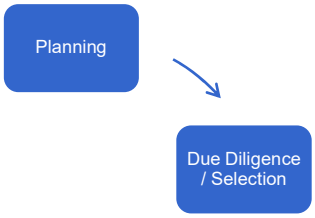
- Assess business and compliance requirements and needs
- Get context
- Identify inherent risk and compliance implications
- Internal cost and value analysis
- Control identification
- Residual risk and risk appetite

NAVEX GLOBAL

 | Page 18

18

Designing an Effective Vendor Risk Process



Due Diligence / Selection

- Mapping capabilities to needs
- Assessing identified quality and risk control capabilities
- Assessing ability to meet compliance obligations
- Assessing costs and value
- Identifying responsibilities
- External validation
  - Include reputational, compliance IT and financial capabilities

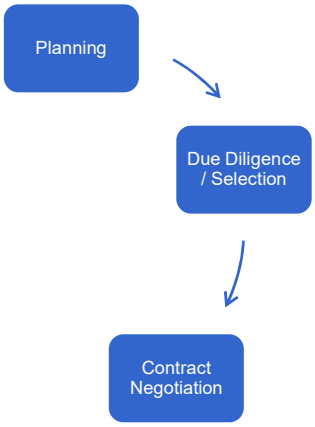
NAVEX GLOBAL

 | Page 19

19

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Designing an Effective Vendor Risk Process



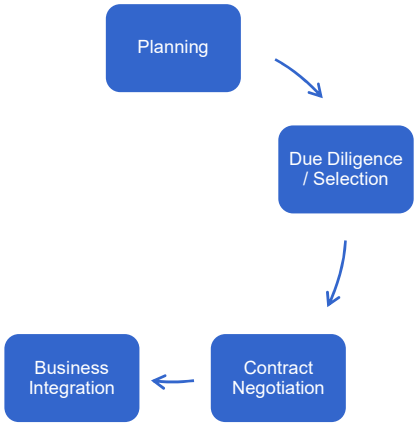
Contract Negotiation

- Compliant pricing relates to value
- Required compliance, quality and risk related controls documented
- Audit process identified
- Service Level Agreements or SLAs
- Responsible, Accountable, Consulted and Informed or RACI Matrices
- Onboarding / testing / business resiliency / BC agreed to
- Data ownership / retention / destruction / purpose
- Insurance
- Status as a vendor or customer

NAVEX GLOBAL

20

Designing an Effective Vendor Risk Process



Business Integration

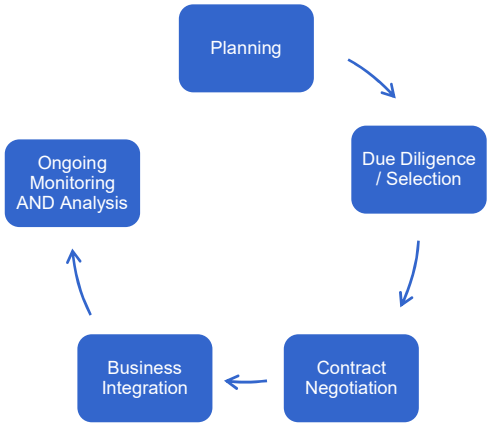
- Onboarding
- Attestation to compliance obligations
- Process mapping
- Deliverable schedules / SLAs
- Business resiliency / continuity planning and testing

NAVEX GLOBAL

21

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Designing an Effective Vendor Risk Process

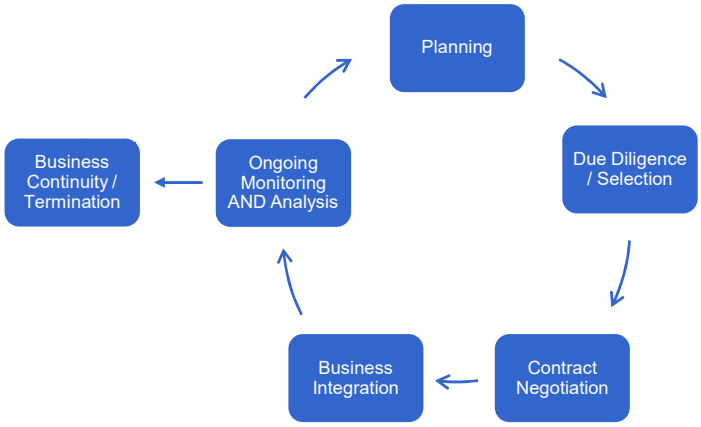


Ongoing Monitoring & Analysis

- Flexible, risk-based scheduling
- Compliance, risk and quality control monitoring
- Assessments
  - SIG, SIG Lite, CAIQ Star, etc.
- Reports & documents
  - SOC I, SOC II, Privacy Policy, etc.
- Third party intelligence
  - RiskRate
  - SecurityScorecard, BitSight, RiskRecon
  - RapidRatings, D&B
  - Vendor news (RSS)
  - KChecks, CORL, SDN, Denied persons, OFAC
- Issues management
- Analysis

NAVEX GLOBAL

Designing an Effective Vendor Risk Process



Business Continuity / Termination

- Business interruption support
- Termination risk & alternatives
  - Purchasing vendor
  - Renegotiating
- Retrieving/disposing assets
  - Data, tools, space, etc.
  - Protecting information

NAVEX GLOBAL

Ongoing Monitoring & Effective Interpretation

NAVEX GLOBAL

 | Page 24

24

Ongoing Monitoring and Analysis: Messaging for Effectiveness

25

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

26

Ongoing Monitoring and Analysis: Messaging for Effectiveness

27

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

28

Ongoing Monitoring and Analysis: Messaging for Effectiveness

29

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

30

Ongoing Monitoring and Analysis: Messaging for Effectiveness

31

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

32

33

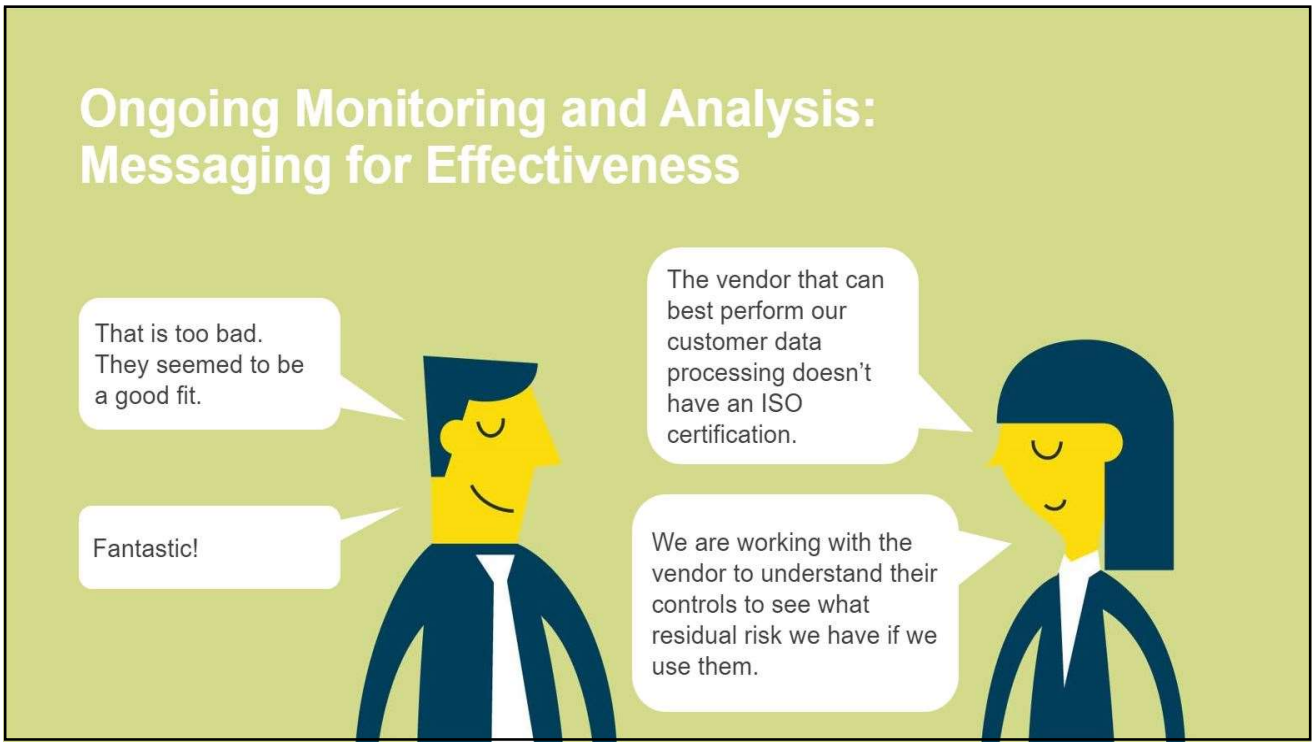
© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

34

35

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

36



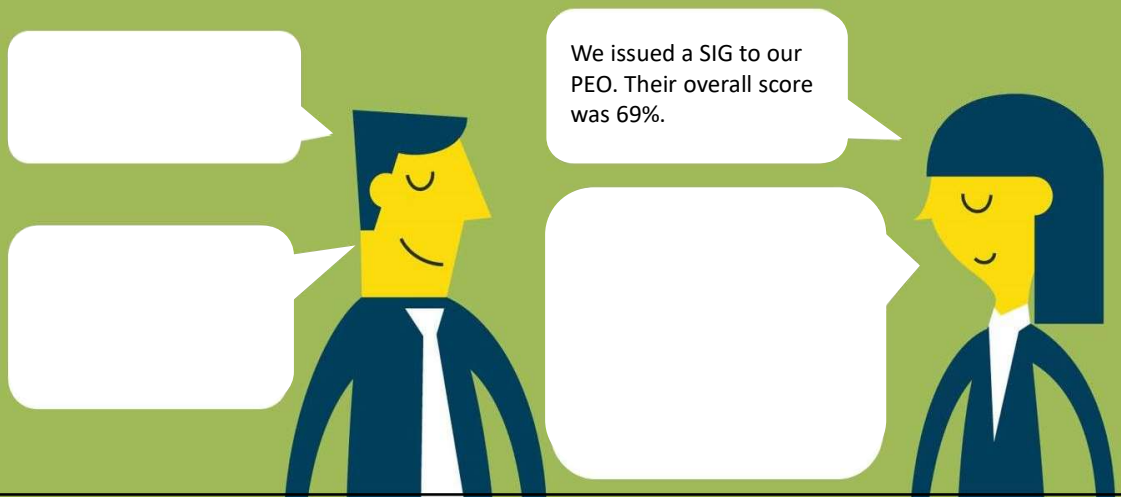
37

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

38

Ongoing Monitoring and Analysis: Messaging for Effectiveness



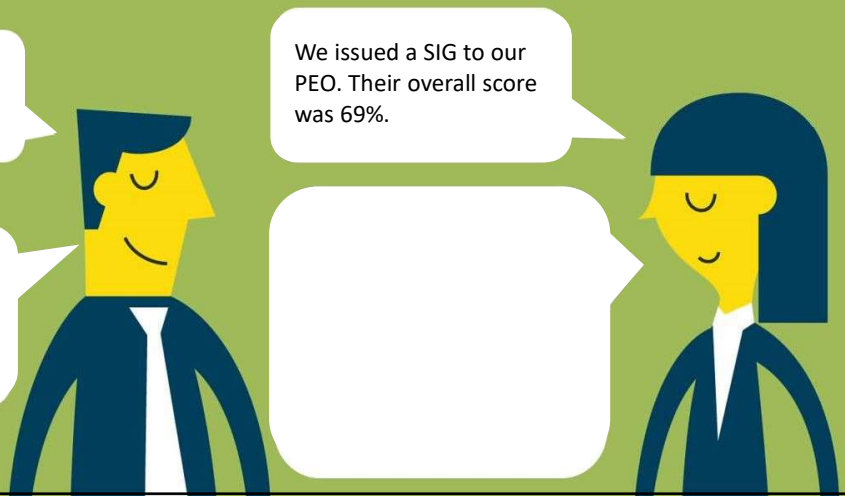
39

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

That seems bad. Guess we need to find a new PEO.

We issued a SIG to our PEO. Their overall score was 69%.



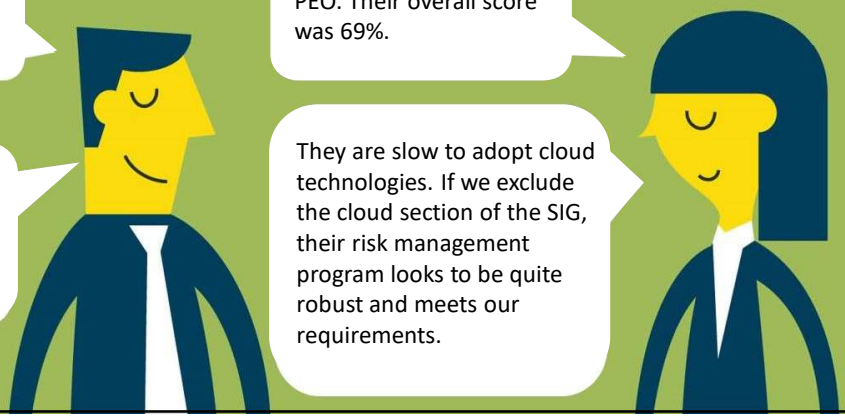
40

Ongoing Monitoring and Analysis: Messaging for Effectiveness

That seems bad. Guess we need to find a new PEO.

We issued a SIG to our PEO. Their overall score was 69%.

They are slow to adopt cloud technologies. If we exclude the cloud section of the SIG, their risk management program looks to be quite robust and meets our requirements.



41

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Messaging for Effectiveness

That seems bad. Guess we need to find a new PEO.

We should probably have them alert us if they mature to using cloud technologies.

We issued a SIG to our PEO. Their overall score was 69%.

They are slow to adopt cloud technologies. If we exclude the cloud section of the SIG, their risk management program looks to be quite robust and meets our requirements.

42

Ongoing Monitoring and Analysis: Messaging for Effectiveness

43

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

44

45

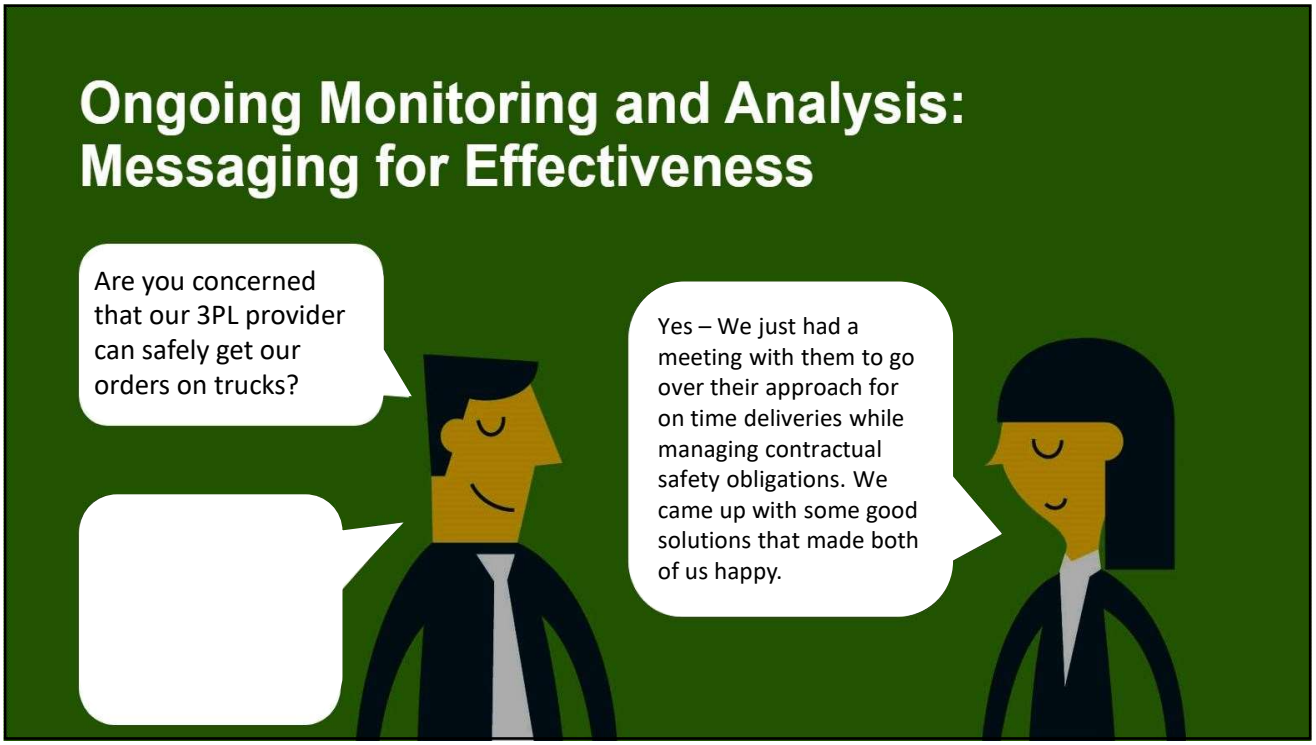
© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

46

47

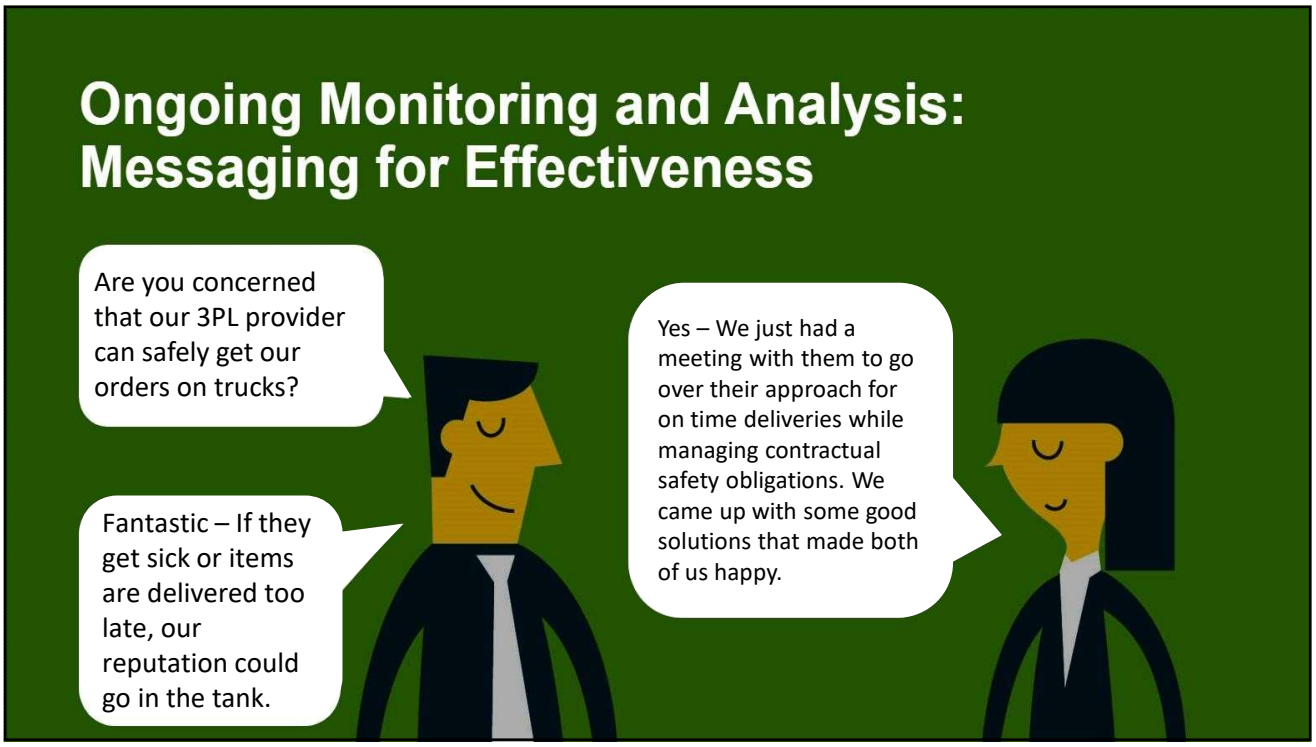
© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

48



49

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›



50

Ongoing Monitoring and Analysis: Risk-Based Approach

One size does not fit all

- Time consuming approach
- Costs often outweigh benefits
- Frustrates vendor relationships
- Creates risk

NAVEX GLOBAL

51

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Ongoing Monitoring and Analysis: Risk-Based Approach

One size does not fit all

- Time consuming approach
- Costs often outweigh benefits
- Frustrates vendor relationships
- Creates risk

Manage and schedule by risk

- Internal assessments
- Privacy assessments
- Vendor assessments
- Control effectiveness
- Concentration assessment
- Key performance indicators and key risk indicators

NAVEX GLOBAL

52

Ongoing Monitoring and Analysis: Risk-Based Approach

One size does not fit all

- Time consuming approach
- Costs often outweigh benefits
- Frustrates vendor relationships
- Creates risk

Manage and schedule by risk

- Internal assessments
- Privacy assessments
- Vendor assessments
- Control effectiveness
- Concentration assessment
- Key performance indicators and key risk indicators

Improve relationships for vendor performance

- Ensure all in process understand goals
- Streamline assessments
- Identify alternatives to achieve control effectiveness

NAVEX GLOBAL

53

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Approach

NAVEX GLOBAL

 | Page 54

54

Toolsets for Privacy and Vendor Risk Management Success

NAVEX GLOBAL

 | Page 55

55

Toolsets for Privacy and Vendor Risk Management Success

Office Tools (spreadsheets, etc)

- Small set of third parties
- Compact organization with simpler operations
- Not a regulated industry
- Limited compliance information being shared
- Low/no examination or external audit demands

NAVEX GLOBAL

56

Toolsets for Privacy and Vendor Risk Management Success

Office Tools (spreadsheets, etc)

- Small set of third parties
- Compact organization with simpler operations
- Not a regulated industry
- Limited compliance information being shared
- Low/no examination or external audit demands

Third Party Point Solutions

- Robust approach to vendor risk management required – even if capabilities are being matured
- Compliance must be managed in one or more jurisdictions
- Messaging needs to be differentiated – including messaging to vendors
- Need for downstream risk information
- Need to manage compliance related issues with vendors

NAVEX GLOBAL

57

Toolsets for Privacy and Vendor Risk Management Success

Office Tools (spreadsheets, etc)

- Small set of third parties
- Compact organization with simpler operations
- Not a regulated industry
- Limited compliance information being shared
- Low/no examination or external audit demands

Third Party Point Solutions

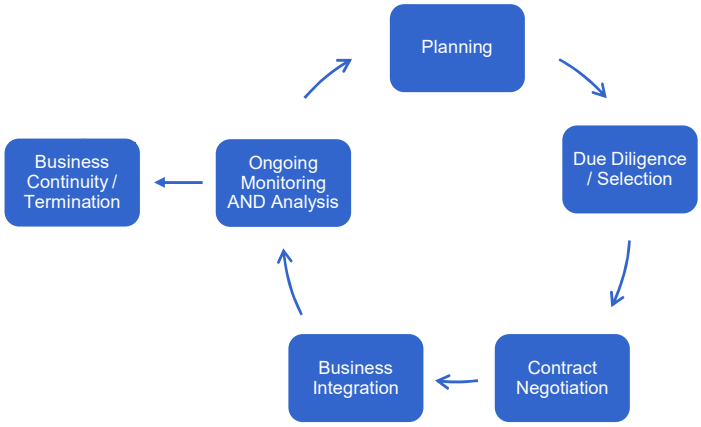
- Robust approach to vendor risk management required – even if capabilities are being matured
- Compliance must be managed in one or more jurisdictions
- Messaging needs to be differentiated – including messaging to vendors
- Need for downstream risk information
- Need to manage compliance related issues with vendors

GRC / IRM

- Robust approach to vendor and operational risk management required – including compliance
- Enterprise wide compliance management including IT risk, and other risk management disciplines as well as incident response and business continuity
- Vendor risk outputs critical to other decisions

NAVEX GLOBAL

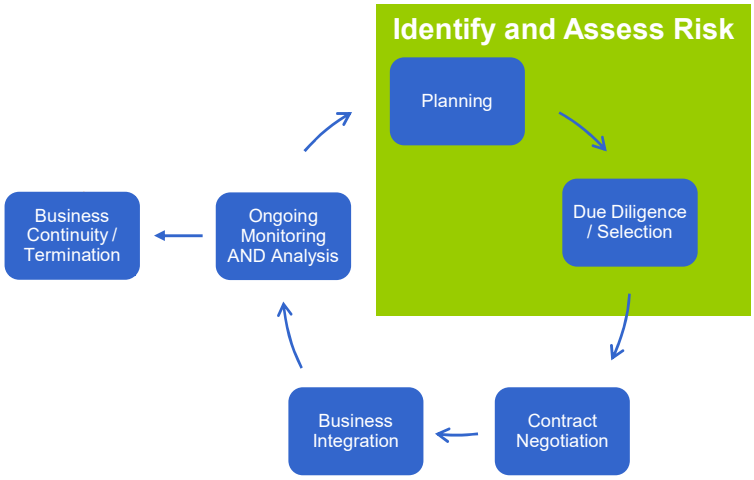
Framework for Risk Management



Vendor risk management follows basic tenants of other risk management frameworks

NAVEX GLOBAL

Framework for Risk Management



Vendor risk management follows basic tenants of other risk management frameworks

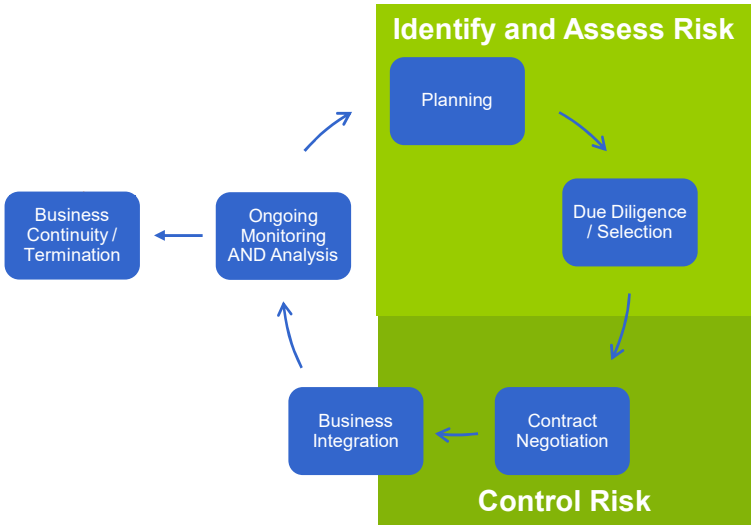
- Assess risk

NAVEX GLOBAL

 | Page 60

60

Framework for Risk Management



Vendor risk management follows basic tenants of other risk management frameworks

- Assess risk
- Control risk

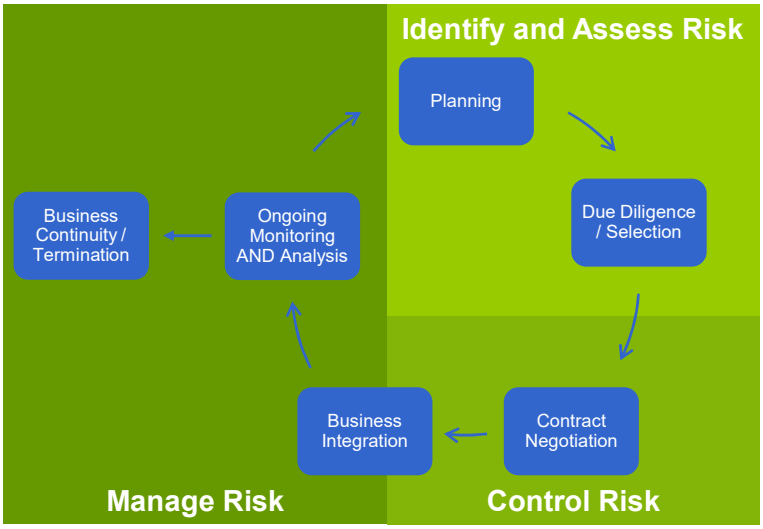
NAVEX GLOBAL

 | Page 61

61

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Framework for Risk Management



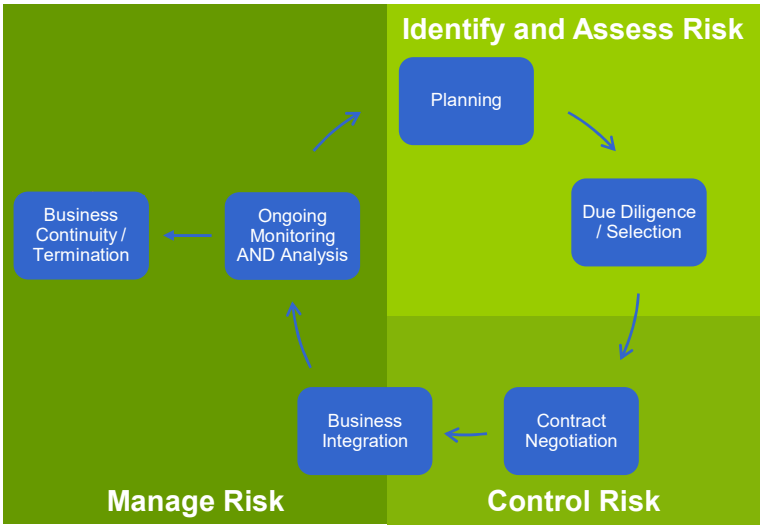
Vendor risk management follows basic tenants of other risk management frameworks

- Assess risk
- Control risk
- Manage risk

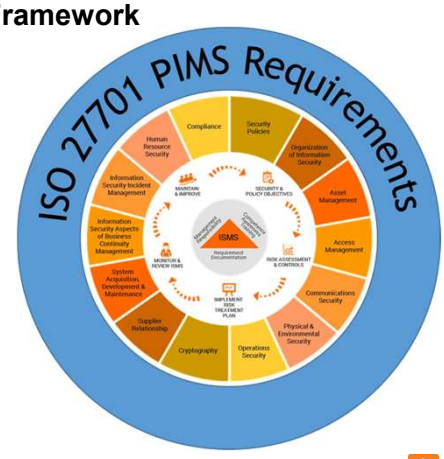
NAVEX GLOBAL

62

Framework for Risk Management



ISO 27701 Privacy Management / ISO 27001 Information Security Framework

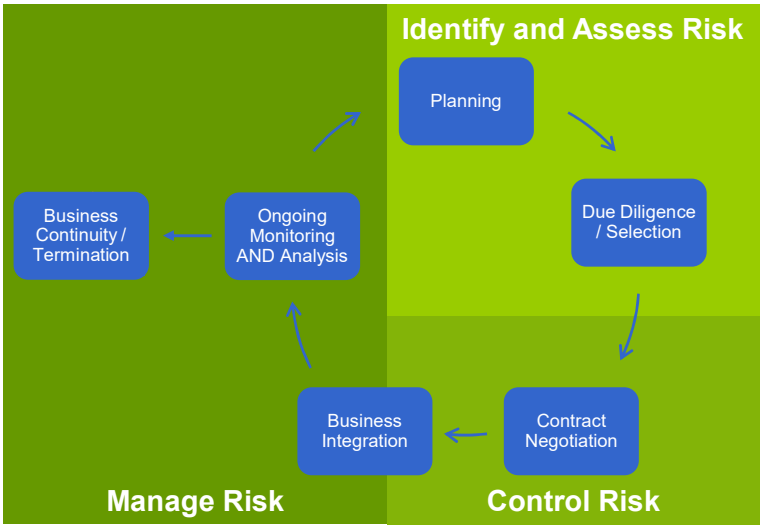


NAVEX GLOBAL

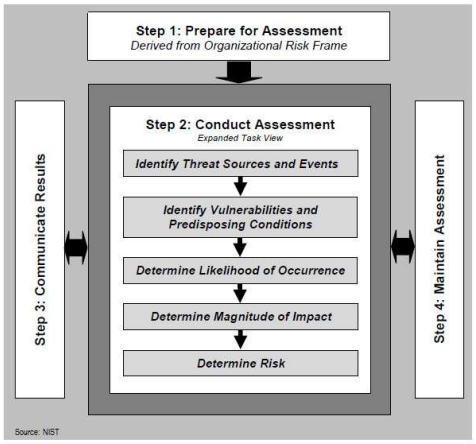
63

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Framework for Risk Management



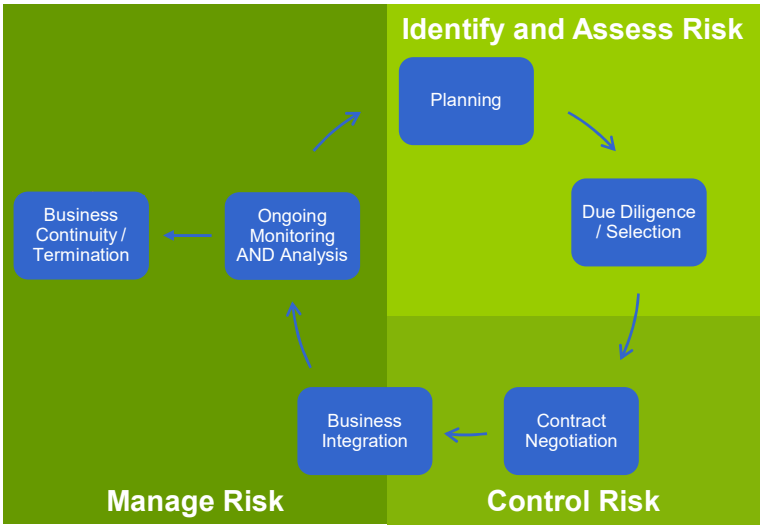
ISO 31000 Risk Management Framework



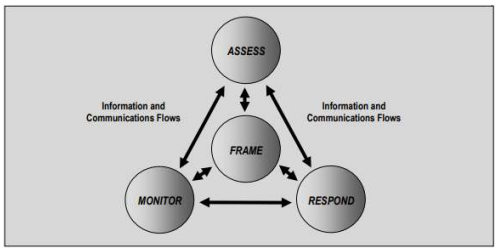
NAVEX GLOBAL

64

Framework for Risk Management



- **NIST 800-39 (referenced in NIST 800-161)**

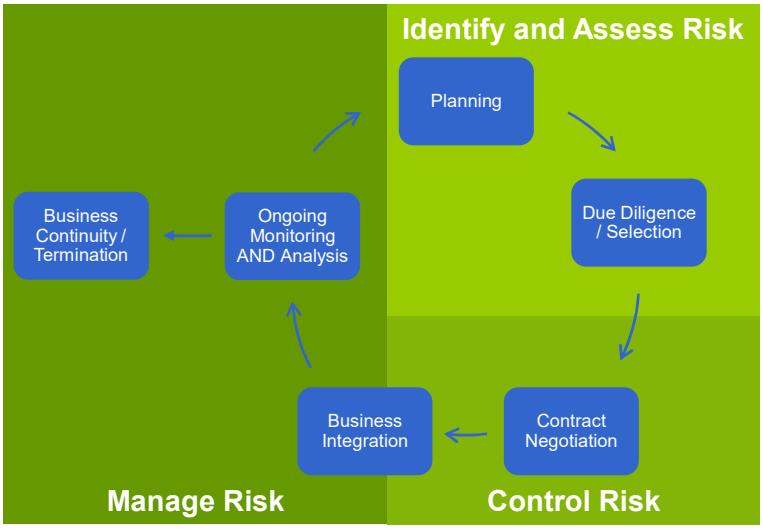


NAVEX GLOBAL

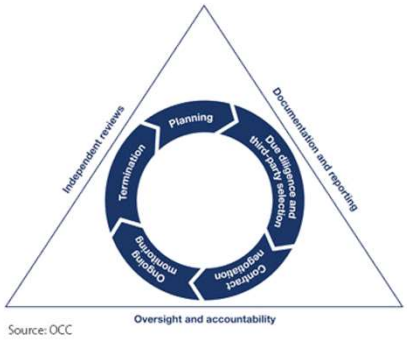
65

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Framework for Risk Management



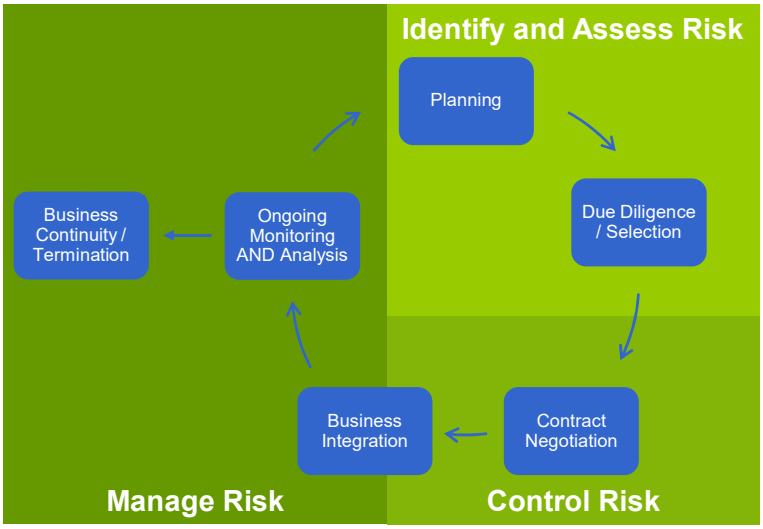
OCC 2013-29, 2017-7, 2017-21



NAVEX GLOBAL

66

Framework for Risk Management



PCI – DSS 3.2.1

Lockpath Third Party Framework	PCI-DSS Tenant
Control Risk	Build and Maintain a Secure Network and System
Manage Risk	Protect Cardholder Data
Control Risk	Maintain Vulnerability Management Program
Manage Risk	Implement Strong Access Control Measures
Manage Risk	Regularly Monitor and Test Networks
Identify and Assess Risk	Maintain an Info Security Policy

NAVEX GLOBAL

67

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›

Thank You.

NAVEX GLOBAL®

 | Page 68

© 2019 NAVEX Global, Inc. All Rights Reserved. | Page ‹#›