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

Sam Abadir, CISM
Director, Industry Solutions – NAVEX Global

Agenda

• Third Party Risk and Compliance Impacts
• Third-Party Risk Framework
• Ongoing Monitoring & Effective Interpretation
• Approach
What Are Third Parties?

- Your organization does not stand alone

Your Organization
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
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.

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?
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?

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

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
Third Parties

• Third parties put your organization at risk — and that risk can ripple throughout the business.
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.
Poll Question

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

- Financial
- Operational
- Reputational
- Regulatory
- Compliance

Third-Party Risk Framework
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

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
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

Designing an Effective Vendor Risk Process

**Business Integration**
- Onboarding
- Attestation to compliance obligations
- Process mapping
- Deliverable schedules / SLAs
- Business resiliency / continuity planning and testing
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)
- Issues management
- Analysis

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

Ongoing Monitoring and Analysis: Messaging for Effectiveness
Ongoing Monitoring and Analysis: Messaging for Effectiveness

Our fulfillment center just showed up on OFAC

Did you just say our vendor is fat?
Ongoing Monitoring and Analysis: Messaging for Effectiveness

Vendor X scored 69% on the SIG.
Ongoing Monitoring and Analysis: Messaging for Effectiveness

Vendor X scored 69% on the SIG.

What is a SIG?

Ongoing Monitoring and Analysis: Messaging for Effectiveness

Vendor Z complies with 64% of our controls.
Ongoing Monitoring and Analysis: Messaging for Effectiveness

Vendor Z complies with 64% of our controls.

Are they important controls?
Ongoing Monitoring and Analysis: Messaging for Effectiveness

The vendor that can best perform our customer data processing doesn’t have an ISO certification.

That is too bad. They seemed to be a good fit.

The vendor that can best perform our customer data processing doesn’t have an ISO certification.
Ongoing Monitoring and Analysis: Messaging for Effectiveness

That is too bad. They seemed to be a good fit.

The vendor that can best perform our customer data processing doesn’t have an ISO certification.

We are working with the vendor to understand their controls to see what residual risk we have if we use them.

Fantastic!

We are working with the vendor to understand their controls to see what residual risk we have if we use them.
We issued a SIG to our PEO. Their overall score was 69%. That seems bad. Guess we need to find a new PEO.

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

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.

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%.

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

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.

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

I saw that our sales brokers are now all working from home. Are we sure they cannot be hacked? They'd have instant access to our network if they were.

We are concerned about this too. We shipped them all hardened laptops to support our work and got extra VPN licenses from our network manager.

Great idea! That allows them to work from home with greater levels of information security.

Do you think I can lease them the laptops they have?
Ongoing Monitoring and Analysis: Messaging for Effectiveness

I saw that our sales brokers are now all working from home. Are we sure they cannot be hacked? They’d have instant access to our network if they were.

We are concerned about this too. We shipped them all hardened laptops to support our work and got extra VPN licenses from our network manager.
Ongoing Monitoring and Analysis: Messaging for Effectiveness

I saw that our sales brokers are now all working from home. Are we sure they cannot be hacked? They'd have instant access to our network if they were.

We are concerned about this too. We shipped them all hardened laptops to support our work and got extra VPN licenses from our network manager.

Great idea! That allows them to work from home with greater levels of information security. Do you think I can lease them the laptops they have?

Are you concerned that our 3PL provider can safely get our orders on trucks?

Yes – We just had a meeting with them to go over their approach for on time deliveries while managing contractual safety obligations. We came up with some good solutions that made both of us happy.

Fantastic – If they get sick or items are delivered too late, our reputation could go in the tank.
Are you concerned that our 3PL provider can safely get our orders on trucks?

Yes – We just had a meeting with them to go over their approach for on time deliveries while managing contractual safety obligations. We came up with some good solutions that made both of us happy.

Fantastic – If they get sick or items are delivered too late, our reputation could go in the tank.
Ongoing Monitoring and Analysis: Messaging for Effectiveness

Are you concerned that our 3PL provider can safely get our orders on trucks?

Yes – We just had a meeting with them to go over their approach for on time deliveries while managing contractual safety obligations. We came up with some good solutions that made both of us happy.

Fantastic – If they get sick or items are delivered too late, our reputation could go in the tank.

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
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

Manage and schedule by risk
- Internal assessments
- Privacy assessments
- Vendor assessments
- Control effectiveness
- Concentration assessment
- Key performance indicators and key risk indicators
Approach

Toolsets for Privacy and Vendor Risk Management Success
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
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

Framework for Risk Management

Vendor risk management follows basic tenants of other risk management frameworks
Vendor risk management follows basic tenants of other risk management frameworks

- Assess risk
- Control risk
Vendor risk management follows basic tenants of other risk management frameworks:

- Assess risk
- Control risk
- Manage risk
Framework for Risk Management

Identify and Assess Risk

- Planning
- Due Diligence / Selection
- Business Continuity / Termination
- Ongoing Monitoring AND Analysis

Manage Risk

Control Risk

Business Integration
Contract Negotiation

ISO 31000 Risk Management Framework

- Step 1: Prepare for Assessment
  - Derived from Organizational Risk Framework
- Step 2: Conduct Assessment
  - Identify Threat Sources and Events
  - Identify Vulnerabilities and Predisposing Conditions
  - Determine Likelihood of Occurrence
  - Determine Magnitude of Impact
  - Determine Risk

• NIST 800-39
(referenced in NIST 800-161)
Framework for Risk Management

Identify and Assess Risk

- Planning
- Ongoing Monitoring AND Analysis
- Due Diligence / Selection
- Business Integration
- Contract Negotiation

Manage Risk

Control Risk

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

Framework for Risk Management

Identify and Assess Risk

- Planning
- Ongoing Monitoring AND Analysis
- Due Diligence / Selection
- Business Integration
- Contract Negotiation

Manage Risk

Control Risk

PCI – DSS 3.2.1

<table>
<thead>
<tr>
<th>Lockpath Third Party Framework</th>
<th>PCI-DSS Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Risk</td>
<td>Build and Maintain a Secure Network and System</td>
</tr>
<tr>
<td>Manage Risk</td>
<td>Protect Cardholder Data</td>
</tr>
<tr>
<td>Control Risk</td>
<td>Maintain Vulnerability Management Program</td>
</tr>
<tr>
<td>Manage Risk</td>
<td>Implement Strong Access Control Measures</td>
</tr>
<tr>
<td>Manage Risk</td>
<td>Regularly Monitor and Test Networks</td>
</tr>
<tr>
<td>Identify and Assess Risk</td>
<td>Maintain an Info Security Policy</td>
</tr>
</tbody>
</table>
Thank You.