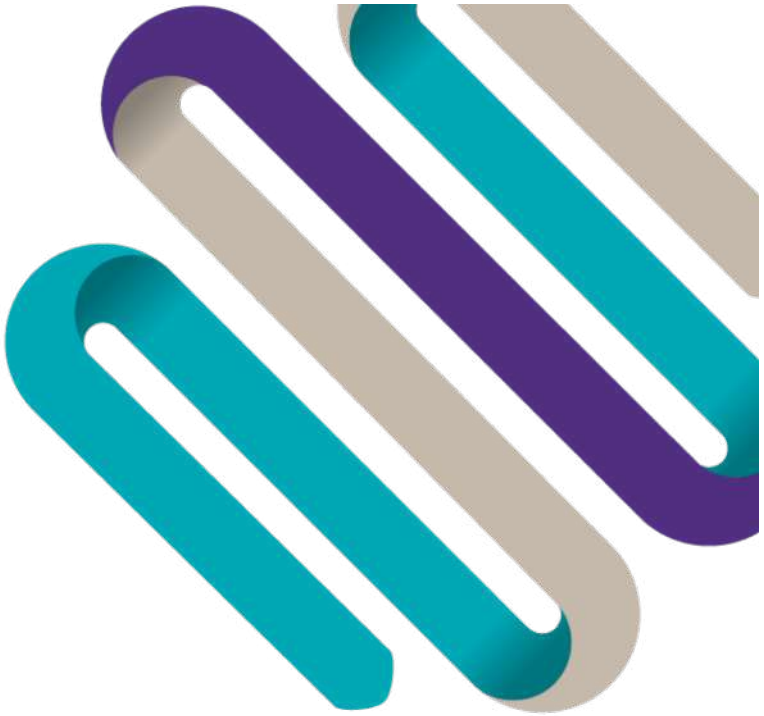


Calculating Inherent Risk – How KeyBank brought Efficiency and Consistency to their Current Program

CEFPRO
Vendor & Third Party Risk USA Conference

June 2018

The World's Most Valuable Resource

Source: 5/16/17 Economist <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>

"Show Me the Data!"

Grant Thornton

Driving Business Value & Managing Risks

Third Party Risk Management Program (TPRM) leaders need to not only manage the expanding risks that third parties can introduce in the organization, but also ensure stakeholders see the value of the program. This requires a delicate balance between senior management support, business enablement and risk management.

- Drive revenue
- Optimize costs
- Innovate
- Service clients

A Balancing Act

- Meet regulatory expectations
- Develop leading practices
- Protect Brand

Not managing third party risks tightly enough may have a negative impact or lead to unanticipated losses and reputational damage

Managing risks too tightly inhibits key partners from growing the business and providing value to their clients and shareholders

Grant Thornton

The Problem

- Each third party engagement requires an individual inherent risk assessment
- Due Diligence requirements are determined after inherent risk assessment is complete
- Subjectivity can create inconsistencies
- Ongoing enhancements to risk assessment create the need to reassess existing third party engagements

Grant Thornton

The Solution: A Service Category Approach

- Each third party engagement requires an individual inherent risk assessment
- Due Diligence requirements are determined after inherent risk assessment is complete
- Subjectivity can create inconsistencies
- Ongoing enhancements to risk assessment create the need to reassess existing third party engagements

- Predefined inherent risk assessments and ratings
- Due Diligence requirements are predefined by category
- Consistency within Service Category
- Enhancements can be applied by Service Category, rather than each individual engagement

Grant Thornton

Methodology

Grant Thornton worked with KeyBank stakeholders, existing historical data and knowledge of financial services risk categories to design a new service category approach to create due diligence efficiencies.

Using a Service Category approach will decrease assessment time and provide greater consistency

1 Develop Profiles: Data Analytics

- Used data analytics to build service risk profiles based on current KeyBank Data
- Validated with focused interviews with key stakeholders
- Evaluated answers to similar responses/ define standards
- Reviewed risk profiles to validate ratings

2 Apply Profiles

Service Category Risk Profiles

Service Type 1	
InfoSec	Low
Compliance	Service Type 2
Privacy	InfoSec: High
	Compliance: Moderate
	Privacy: High
	AML: Low

ILLUSTRATIVE

3 Determine Inherent Risk Rating

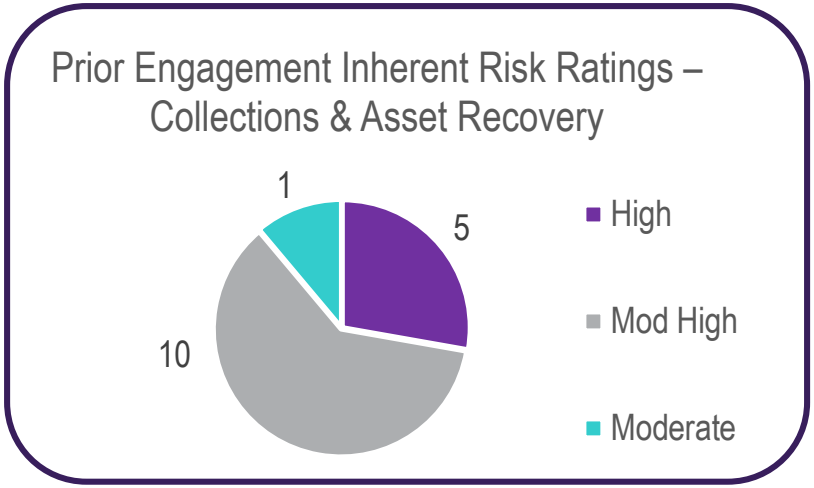
Risk Rating	
5	High
4	Mod-High
3	Moderate
2	Low-Mod
1	Low

4 Map to Due Diligence Routines

Grant Thornton

An Example: Collections & Asset Recovery

1. Extracted Engagements from Archer (GRC)
2. Reviewed and analyzed Engagement Types
3. Assessed which third parties have been routinely risk assessed
4. Determined and reviewed services provided



Grant Thornton

An Example: Collections & Asset Recovery

- **Definition:** This includes collections agencies, repossessions, legal/litigation services, auction services, or information exchanges that facilitate collection-related activities. This excludes software that supports collections activities.
- **Risk Categories**: Compliance, Operational, Information Security, Reputation & Strategic
- **Inherent Risk Rating**: Moderate High

Due Diligence / Ongoing Monitoring Requirements

- Insurance Review
- Financial Viability Assessment
- Compliance Reviews, including Privacy and Fair and Responsible Banking
- Information Security on site evaluation and assessment review
- Litigation and News Searches
- Other internal items such as SLA monitoring, Transition Strategy, and ongoing account meetings

Grant Thornton

Value Add of a Service Category Approach

1. Time Saving!
2. Ties to Authoritative Sources with ability to adjust to regulatory changes quickly across portfolio
3. Consistency in identification of and ties to Risks and Controls
4. Can begin Due Diligence reviews quickly without the wait time for inherent risk calculation
5. Removes subjectivity from risk assessment and provides greater consistency to inherent risks by category of third party activity
6. Identification of required contract language by service type (must have contract terms vs. nice to have)
7. Simplification of identifying entity concentration risk (% of the bank's activity with a particular third party)

Wrap Up

- Operationalized three Service Categories to date
  - Removes need to reassess over a dozen third party engagements
  - Used 3 times already for new third party engagements (in just one month)
- Target is 70 – 100 total Service Categories
- Not all third party engagements will fit into Service Categories
- Reception has been favorable by Program stakeholders

"These predefined service categories are intended to expedite the risk assessment process for Key's onboarding of third parties. ***You can count on Compliance and its TPM Risk Partners to actively contribute to this important project*** *including, but not limited to, providing unfiltered feedback and suggestions. We share in the collective goal described by Grant Thornton as "to bring clarity and consistency to the inherent risk ratings and due diligence requirements in a more efficient manner."*

Grant Thornton

Contact Information

Dennis Frio | Managing Director,
Risk Advisory Services
D +1 646 825 8470
M +1 973 747 2281
E dennis.frio@us.gt.com

Ash Rao | Consultant
D +1 215 531 8731
E ash.rao@us.gt.com

Bob Koszkalda | Director of
Third Party Risk Management
D +1 216 471 2620
E Robert_Koszkalda@KeyBank.com

Jenny Faivre | Third Party
Management Strategist
D +1 216 689 0256
E jenny_r_faivre@KeyBank.com