Constructing an End-to-End Third-Party Risk Management Framework

March 19, 2018

Leith W. Kaplan
leithkaplan@gmail.com

Key Takeaways

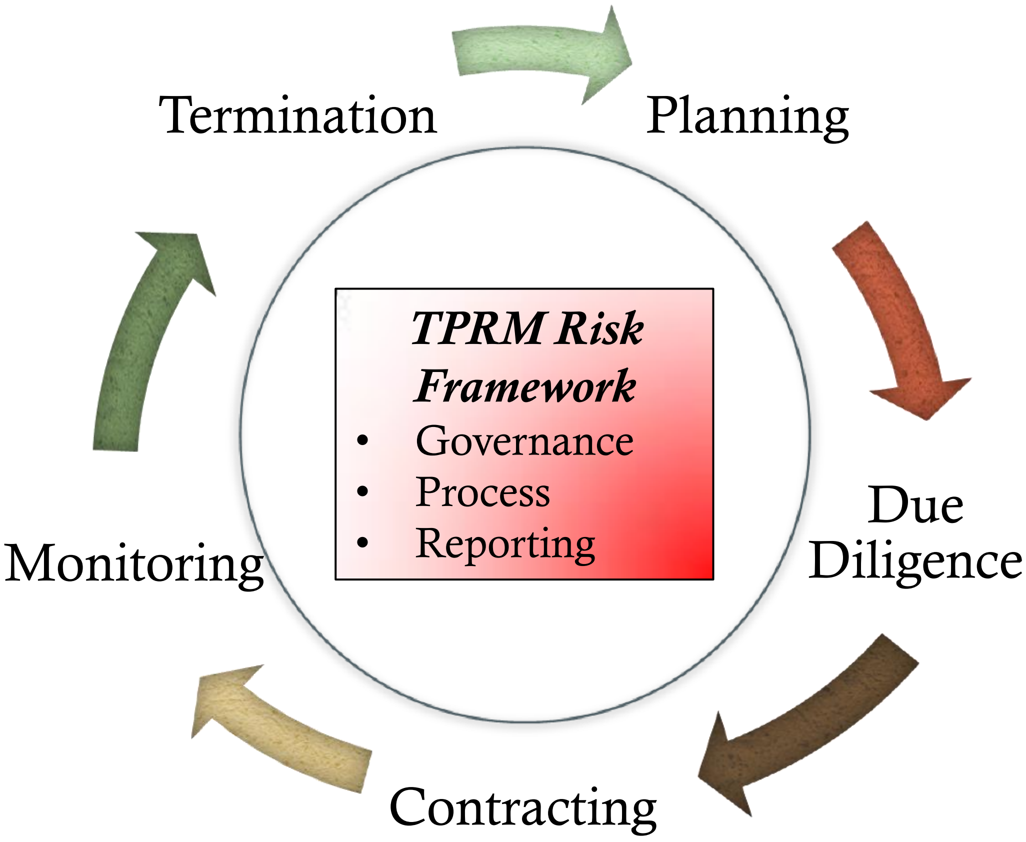
1. There is no one size fits all approach to Third-Party Risk Management (TPRM).

2. An effective TPRM program requires "buy in" throughout the enterprise and alignment of resources across all three lines of defense.

3. Design a TPRM operating model that strives for effectiveness rather than perfection.

4. Assessing third-party risk is a dynamic process and requires continuous monitoring and re-evaluation – simplify and prioritize!

Aligning Risk Framework to Third Party Lifecycle Activities



TPRM Risk Framework

- Governance
- Process
- Reporting

TPRM Governance Considerations

- Governance provides the strategic direction for the entire TPRM target operating model.

- Target operating model defines how the TPRM program will operate taking into account:
  - ✓ Regulatory guidance
  - ✓ Organizational structure and resources across all 3 lines of defense
  - ✓ Business priorities
  - ✓ Risk tolerances
  - ✓ Best practices

- <u>Tip</u>: TPRM success is inextricably linked to delivering "<u>value</u>" – focus on what's most important <u>now</u>!

TPRM Targeted Operating Model

1. Aligning TPRM with enterprise and operational risk management

2. Defining governance structure across 3LOD

3. Policies & Procedures

4. Program Management

5. Practices aligned to third-party life cycle activities
   - Planning, Due Diligence, Contracting, Monitoring Performance & Termination
   - Who does what? When?

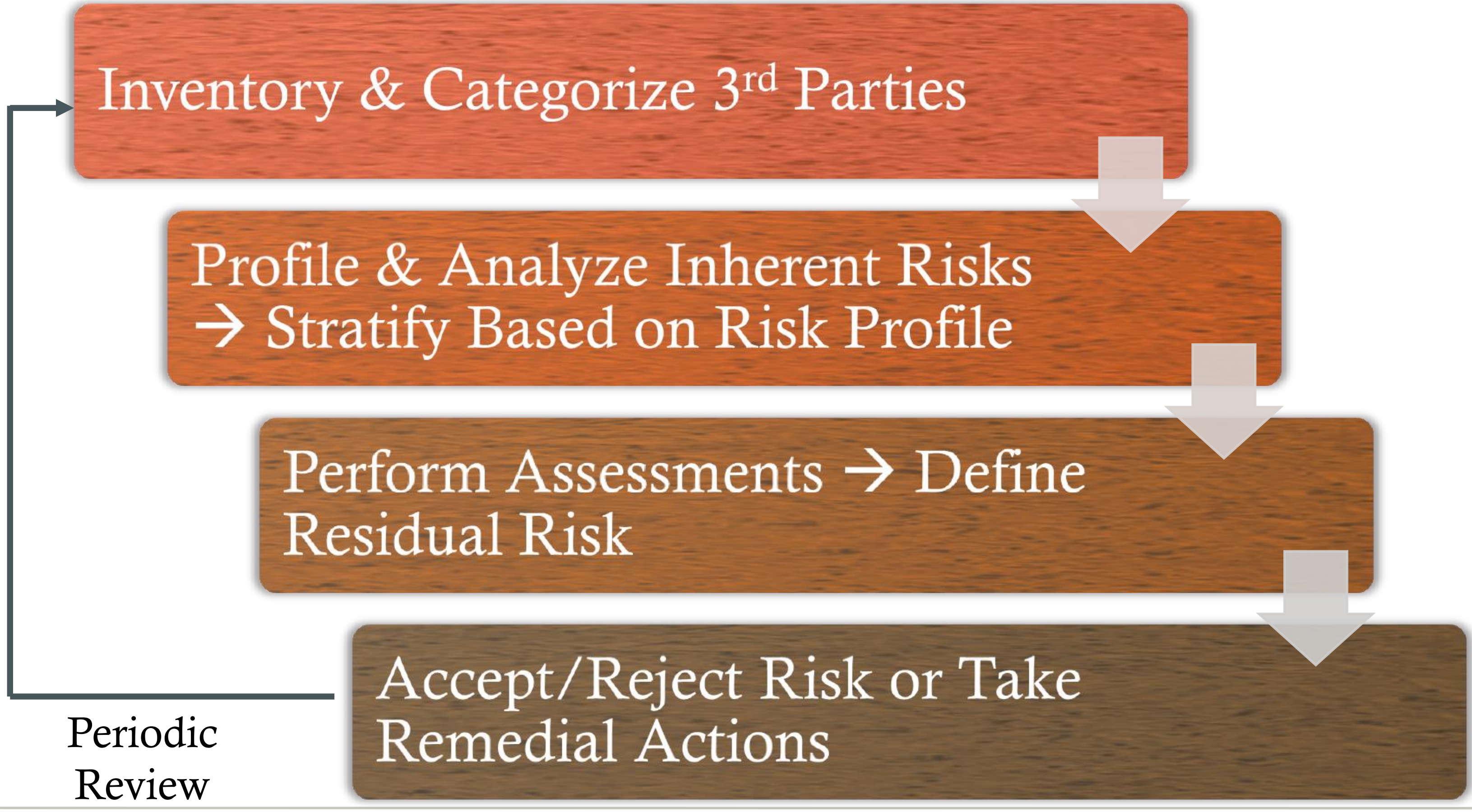
6. Reporting, resources and technology to enable efficiency and effectiveness

Good TPRM Governance = Whatever Works Best

Consider all Stakeholders – Define Roles

3rd Line of Defense	Board of Directors	Risk Committee (as applicable)
	Audit Committee	Internal Audit
2nd Line of Defense	Executive Risk Committee	ERM, Operational Risk
	Legal & Compliance	General Counsel, CCO
	Sourcing & Procurement	CFO, COO, Finance
	Subject Matter Experts	IT, Info Sec, HR, Credit, BCP
1st Line of Defense	Business Units	Internal Clients
		1st Line Risk Managers Vendor Management

Third Party Risk Assessment: Process Overview



Inventory & Categorize 3rd Parties

Profile & Analyze Inherent Risks → Stratify Based on Risk Profile

Perform Assessments → Define Residual Risk

Accept/Reject Risk or Take Remedial Actions

Periodic Review

Develop a “Complete” Inventory of 3rd Parties

Where to Start:

1. Current list(s) of 3rd parties
2. Look to contract inventories
3. Analyze who is paying paid – Accounts Payable
4. Meet with stakeholders and document responses

Scope broadly and narrow focus based on risks!

Is the Inventory Complete?

- Have you conducted an E2E enterprise review of all 3rd party relationships?
  - ✓ Service providers, suppliers, consultants, JV partners, affiliates, brokers, marketing partners, law firms/professionals, correspondent banks, regulated entities…
- Have you considered all applicable requirements?
  - ✓ *Example*: NYDFS Cyber regs include certain employee data under the definition of "nonpublic information".
  - ✓ *Implication*: Service providers with employee data (e.g., recruiters, background check providers, HRIS/Payroll providers) require 3rd party oversight.

Considerations & Roadblocks

- Creating common categories of 3rd party types will simplify risk profiling/assessment activities and enable the creation of baseline due diligence requirements and contract templates.

- Special 3rd parties may be identified that do not neatly fit the existing operating model (e.g., affiliates, "downstream" mortgage foreclosure attorneys).
  - ✓ Tip: Follow 80/20 Rule and leave for resolution later.

- Push back may come from areas not already within the TPRM framework.
  - ✓ Should a roadblock emerge, refer back to applicable requirements and your risk appetite.

What is your (3rd Party) Risk Appetite?

Big Four Accounting Firm Deloitte Confirms Cyber Attack Fortune (Sept 16, 2017)

Law Firm DLA Piper Reels Under Cyber Attack, Fate of Files Unclear Fortune (June 29, 2017)

Equifax data breach: How do you fix a cataclysmic crisis? USA Today (Sept 18, 2017)

Common Risk Domains Requiring Assessment

Risk Domain	Assessing Risk of Loss
Reputational	Impact to the organization based on services provided
Operational	Service criticality, competency to provide services, adequacy of technology and use of 4th parties
Financial	Stability to continue to perform services
Resiliency	Ability to perform in the event of a disaster
Strategic	Competitive considerations; geo-political risks
Info Security	Cyber, privacy, physical security, data integrity
Compliance	Ability to comply with all Requirements

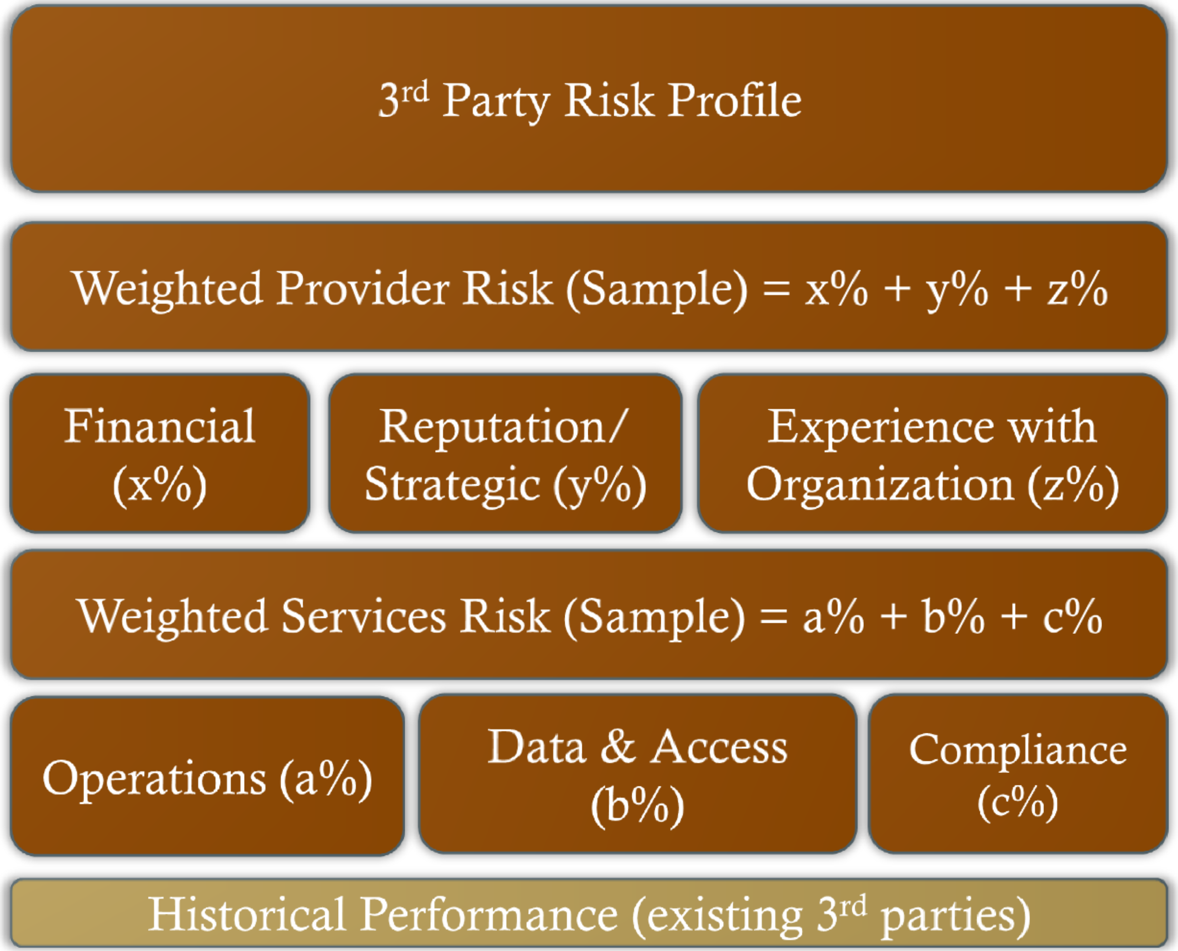
3rd Party Risk Stratification

- Risk stratification focuses TPRM resources on the relationships that matter most (i.e., those with the greatest risk).
- Resulting stratification prioritizes and informs subsequent 3rd party risk assessment activities – depth and frequency.
  - ✓ Area of examiner focus for highly regulated entities (e.g., OCC Bulletin 2013-29).
  - ✓ Using a High-Med-Low scale may not adequately differentiate risks amongst 3rd parties.
  - ✓ Higher risk relationships can be differentiated using a "critical" label to designate riskiest relationships.

Risk Stratification Drives 3rd Party Risk Profile

Sample Stratification Criteria

- Business criticality
- Dollar spend
- Customer impact
- Access to sensitive data
- Systems/Site access
- Offshore location
- Compliance (PCI, GDPR, SOX/SAE 16, BSA/AML)
- Concentration risk***



3rd Party Risk Profile

Weighted Provider Risk (Sample) = x% + y% + z%

Financial (x%)

Reputation/ Strategic (y%)

Experience with Organization (z%)

Weighted Services Risk (Sample) = a% + b% + c%

Operations (a%)

Data & Access (b%)

Compliance (c%)

Historical Performance (existing 3rd parties)

Risk Stratification Decisions: Quantifiable & Defensible

3rd Party Risk = Provider Risk + Service Risk

- Stratification criteria enables an efficient 3rd party risk scoring.
  - ✓ Categories of 3rd parties that do not pose risk should be considered for elimination from TPRM oversight.
  - ✓ Highest risks require greatest time and resources to assess.

- Within each risk criterion, a weighting can be applied to reflect the significance of the risk posed.
  - ✓ <u>Example</u>: In the outsourcing category, greater weighting would be applied to service risks such as customer interaction, access to data and regulatory compliance.

- Effective initial and ongoing risk scoring should always involve the business sponsor.
  - ✓ Effective risk stratification decisions must make sense and be defensible to internal and external stakeholders.

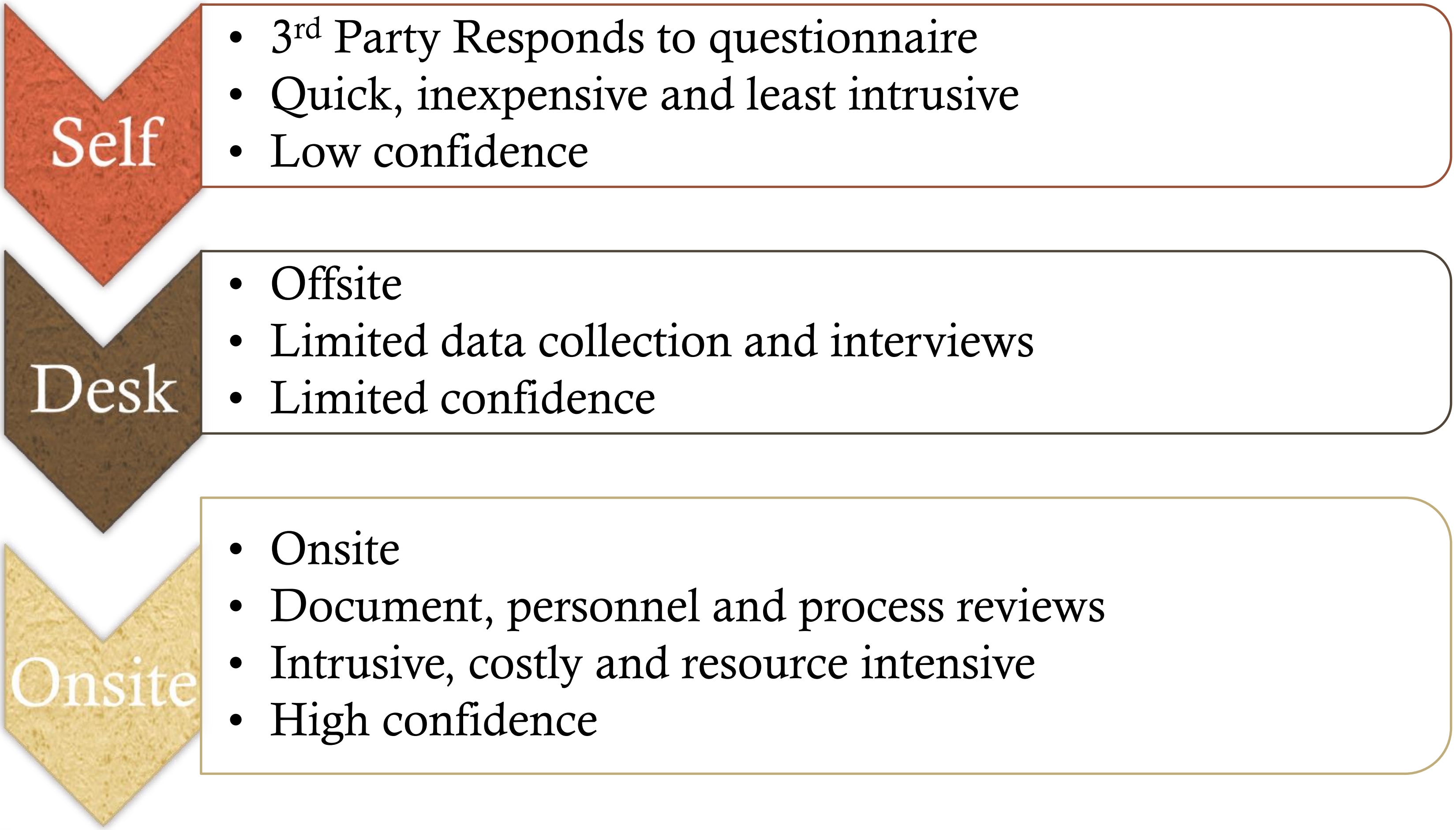
Identifying the Riskiest 3rd Parties

- 3rd Party risk is dynamic – once a critical risk not always a critical risk!

- The highest risk rated 3rd parties should have the following characteristics in common:
  1. A sudden service disruption would have a material adverse impact on the organization.
  2. A service disruption would negatively impact customers.
  3. The 3rd party typically would need more than a day to recover from a service disruption.

- Tip: If more than 10% - 15% of the 3rd parties are ranked in the highest risk category, it may be time to revisit the process.

Typical Assessment Approaches



Self

- 3rd Party Responds to questionnaire
- Quick, inexpensive and least intrusive
- Low confidence

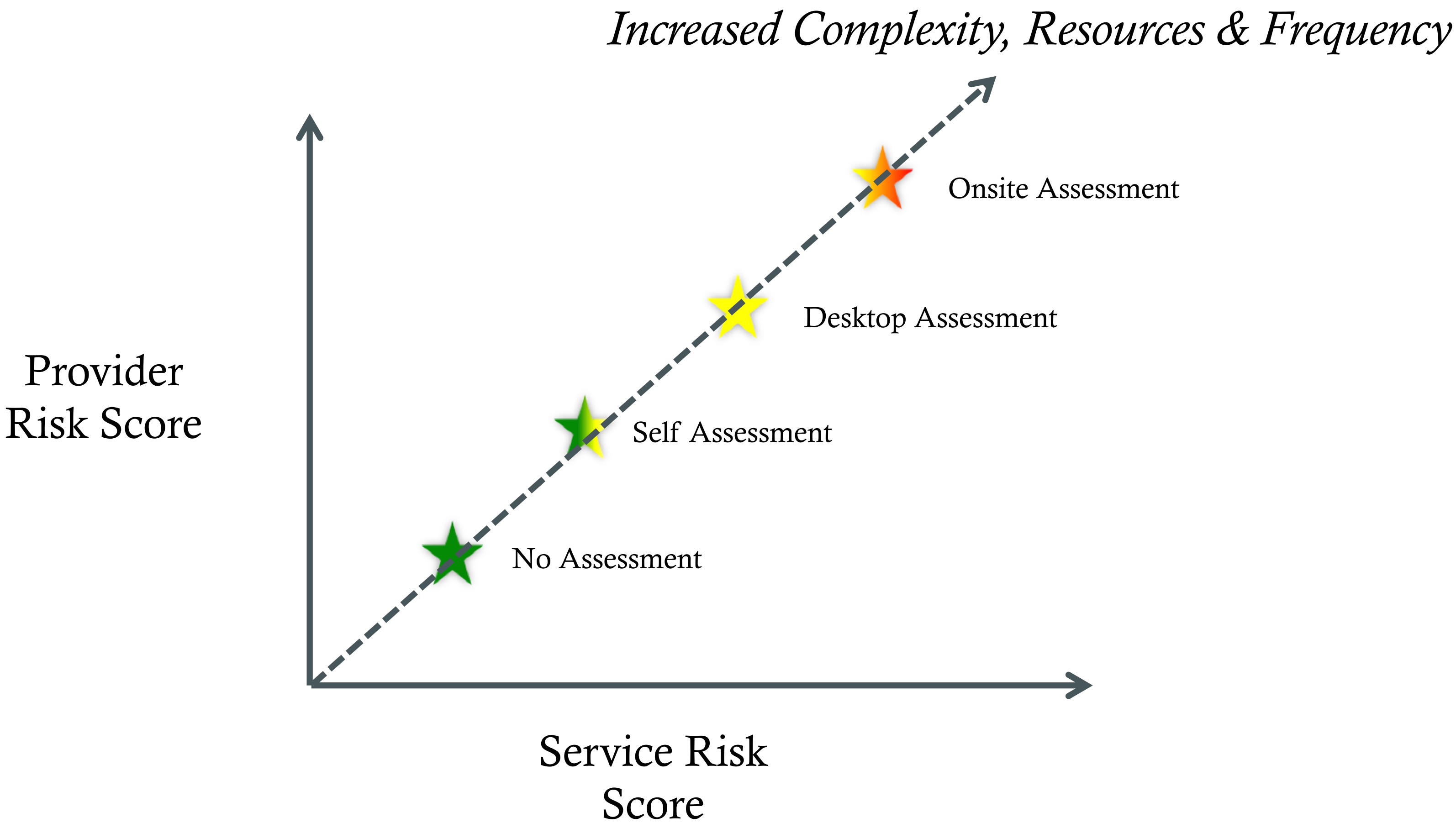
Desk

- Offsite
- Limited data collection and interviews
- Limited confidence

Onsite

- Onsite
- Document, personnel and process reviews
- Intrusive, costly and resource intensive
- High confidence

Effective & Efficient Assessments



Executing the Risk Assessment

- Assessments should take place during the due diligence process and periodically after go-live.
  - ✓ Assessments during initial due diligence can slow the onboarding process if all stakeholders are not aligned.
  - ✓ Frequency of periodic assessments to be driven by residual risk rating.
    - o Example: Critical Risk (6-12 mos.); High-Med Risk (12-18 mos); Med Risk (18-24 mos.); Low (<24 mos.)
- Align the necessary resources and subject matter experts; set expectations accordingly!
- Risk scoring decisions should be updated regularly based on changes related to the provider or services rendered and, as a best practice, at least every 12 months.

Considerations in Executing an Effective Initial Assessment

1. "Mission Critical" requirements (e.g., PCI compliance) should be vetted during the RFP/RFI phase to avoid last minute surprises.

2. Business owner/procurement needs to set upfront due diligence expectations with the counterparty.
   - ✓ Tip: Complaints about diligence burdens could be a red flag.

3. Assess only controls relevant to the services actually rendered. Start with a checklist but don't be beholden to it!

4. Recognize that 3rd parties typically will share evidence demonstrating the existence of controls (e.g., policy requiring annual penetration test) and not necessarily the effectiveness of such controls (e.g., the results of the penetration test).

Considerations in Executing an Effective Initial Assessment

5. What reliance on control effectiveness reports or entity ratings from independent parties (e.g., SSAE 16, USAP) is appropriate?

6. Ongoing control and right to audit requirements need to be imbedded into the underlying contract.
   - ✓ Can/will the 3rd party comply? If so, at what cost?

7. Adherence to P&Ps should facilitate an efficient assessment process – if they do not, revisit them.

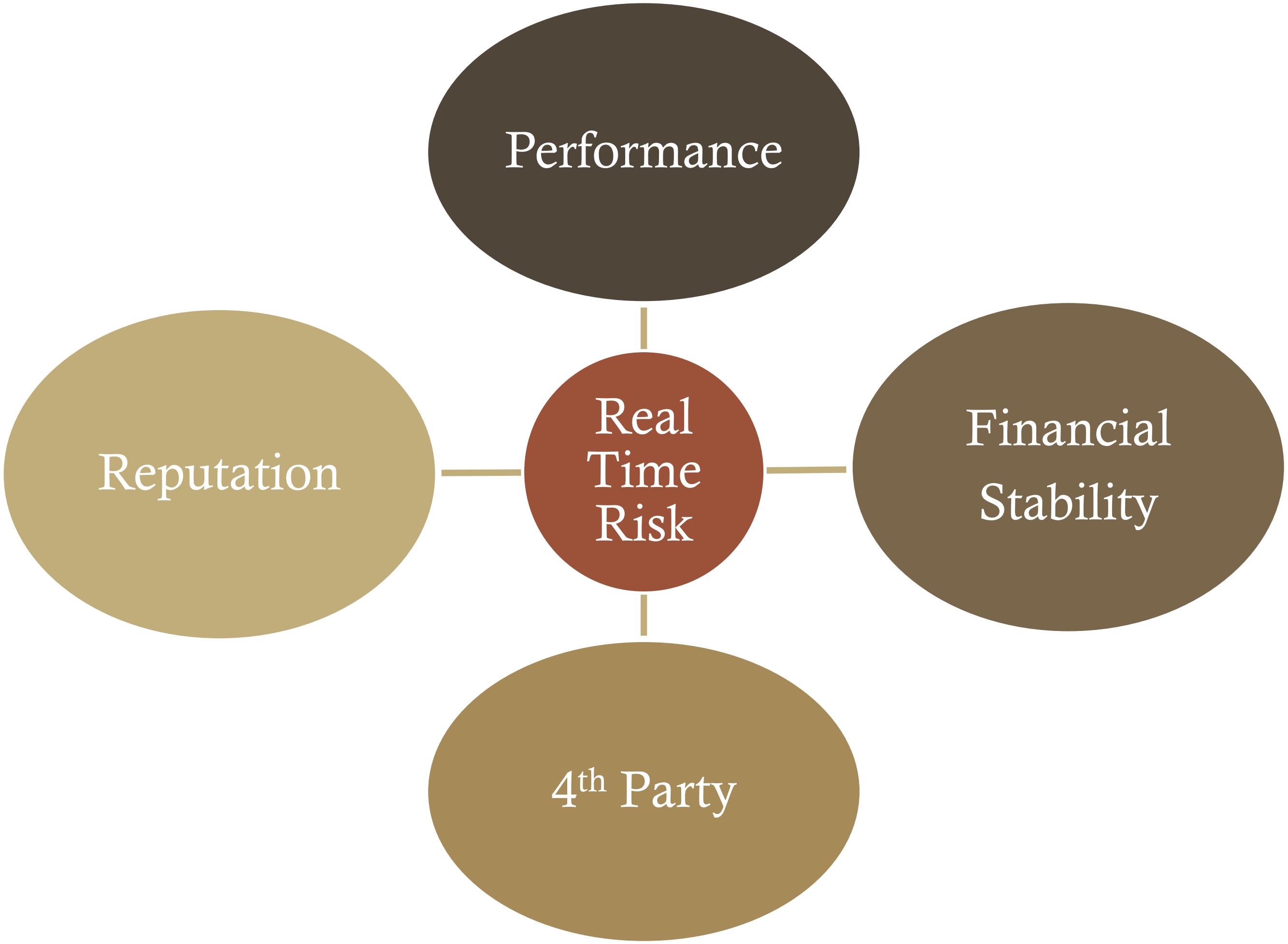
8. The output of the assessment should produce a go/no-go decision and outline any subsequent conditions/remediation.
   - ✓ Tip: High frequency of risk acceptance decisions is an indicator that the TPRM program may not be calibrated to Risk Appetite.

Assessing Control Effectiveness

What level of assurance do you need/require?

- 3rd party controls are an extension of your control environment.
- Controls likely will be different, so how do you assess effectiveness?
  - ✓ If possible, map controls to standardized frameworks (e.g., PCI, ISO, NIST) or regulatory requirements.
  - ✓ Scrutinize the control evidence.
  - ✓ Rely on skill and judgment of your subject matter experts.

“Real Time” Ongoing 3rd Party Risks



Performance

Reputation

Real Time Risk

Financial Stability

4th Party

“Real Time” 3rd Party Risk Monitoring

- An effectively integrated TPRM program should enable the enterprise to understand how their 3rd parties are performing at any given time.
- TPRM framework and P&Ps should clearly address how “real time” operational risks are being monitored and by whom.
- TPRM Program must include standardized processes to identify, escalate, remediate and track 3rd/4th party specific issues to resolution.
  - ✓ TPRM Framework should include triggers for risk re-evaluations in the event of “significant” events.

Risk Reporting

- Reporting should be based on the needs of management, TPRM and Board, but be explainable to regulators.

Management Metrics (KPI)	TPRM (KRI/KPI)	Board
• Quality • Customer Exp. • Service & Delivery • Staffing • Trending • Cost efficacy	• # of Critical 3rd Parties • # of 3rd Parties with access to NPI • Open issues by 3rd party • Assessment turn times	• Top Line KPIs and KRIs • Trending data • Material issue escalation

TPRM Resourcing

✓Right People

✓Right Process

✓Right Technology