THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

RSM

VENDOR MANAGEMENT

Risk mitigation strategies for third party relationships

VGFOA October 2016

INTRODUCTION

Presenters

Lou Cannon, CPA

Public Sector Partner, Assurance Services

Lou has over 35 plus years of experience providing accounting, audit and consulting services to clients in the public sector. Throughout his career he has led and been part of teams conducting operation and performance audits, investigations, compliance, A-133 and financial audits.

Clara Ewing, CIA

Public Sector Director, Risk Advisory Services

Clara has over 15 years of public accounting and consulting experience specializing in internal audit and consulting services for Public Sector clients. She spends 100% of her time as the internal audit Director working with numerous large Counties, Cities and K-12 School Districts.

Agenda

- Walkthrough of the third-party relationship management (TPRM) lifecycle
- Discuss how the Three Lines of Defense model applies to third-party relationships
- Explore the TPRM Maturity Continuum framework and its application to your entity
- Walkthrough of the RSM Vendor Assessment Program's methodology, including our typical approach to risk assessment and project execution

RSM

Third-Party Relationships – Who Are They?

A third-party relationship is any business arrangement between an organization and another entity, by contract or otherwise.

Examples of Third-Party Relationships	
Vendors	Suppliers
Distributors	Licensees
Customers	Professional Service Providers
Subcontractors	Service Contractors
Contract Manufacturers	Business Partners
Brokers	Resellers
Agents	Non-Contractual Parties (e.g. UPS)

RSM

The Increasing Importance of TPRM

The following factors contribute to the need for a strong, demonstrable TPRM:

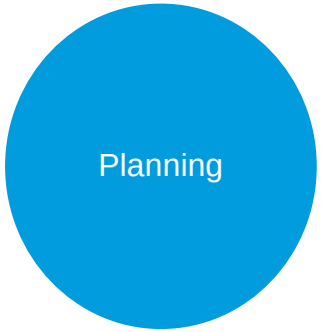
- Recent business changes:
  - Mergers
  - Acquisitions
  - Enterprise-Wide Technology Deployment (i.e. ERP software)
- Increased importance of global sales and supply chains
- High turnover in third-party relationships
- Known third-party data breaches or breach of contract
- Increased offshoring / outsourcing activity
- Off-shoring of key data (financial, operational, sensitive)
- Lack of a solid baseline for third-party risks

RSM

Third-Party Relationship Management (TPRM) Lifecycle

TPRM - Planning

Identifying who your stakeholders are and effectively engaging them throughout the planning process is the best way to ensure objectives and expected outcomes are defined and appropriate third-parties are targeted and procured.



- Need
- Specifications
- Define population of third-parties
- Develop list of qualified third-parties
- Develop RFP
- Manage bid process

TPRM – Due diligence and selection

Creating transparency through timely, complete, and accurate procurement phase documentation is the most effective way to reduce the risk of bid protests and real or perceived instances of favoritism or bias.

Due diligence and third-party selection

- Bid evaluation
- Evaluate qualifications
- Third-party selection

TPRM – Contracting

Identification of inherent risks to the planned third-party relationship is an exercise that should be contemplated during planning and reevaluated during each phase of the TPRM lifecycle. An effective contract seeks to balance these risks evenly amongst the executing parties.

- Third-party negotiations
- Critical elements of agreement
- Contract development and final signature

RSM

TPRM – Ongoing monitoring

Regardless of how well an organization plans, procures, or contracts with a third-party, regular monitoring of vendors is critical to ensuring the objectives and expected outcomes of the relationship are achieved.

- Contract administration
- Initial deliveries
- Continued delivery
- Payments
- Quality controls
- Performance metrics and feedback
- Compliance audits
- Insurance verification
- IT security and privacy

TPRM – Termination

An effective transition from one vendor to the next requires proper planning, and is largely contingent upon collaboration and transparency between the outgoing provider, incoming provider, and management.

- Contract termination and expiration
- Contractual termination requirements
- Final audit and settlement
- Legal closure
- Post-mortem review and lessons learned

RSM

Three Lines of Defense Model

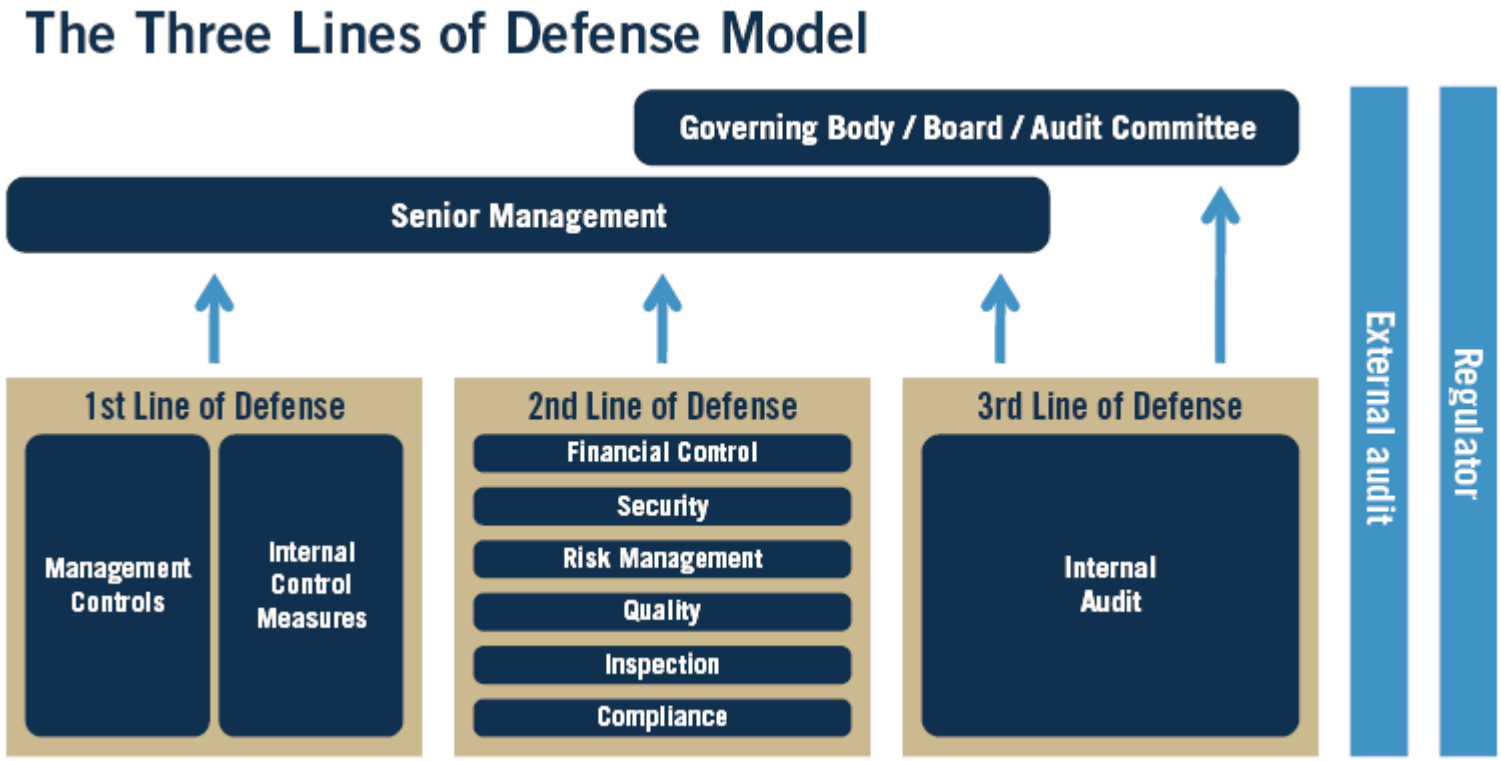
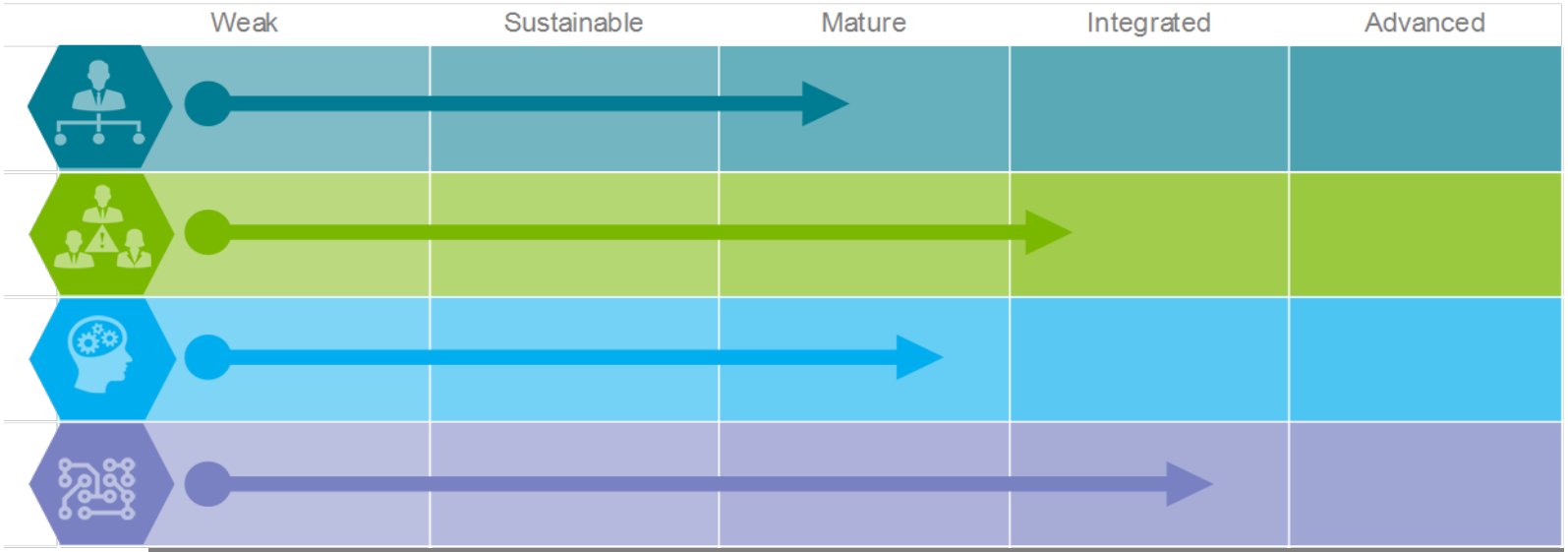


Image used with permission by the Institute of Internal Auditors

TPRM Maturity Continuum



Weak

- Ad-hoc processes
- Problem driven
- Inconsistent outcomes
- Rework
- Reactive
- Individual effort

Sustainable

- Basic process
- Processes follow a regular pattern
- Repeatable practices
- Reduced rework
- Processes not standardized

Mature

- Documented processes
- Standard approval processes
- Proactive and reactive
- Request driven
- Technology utilized
- Improve productivity

Integrated

- Stable processes
- Proactive
- Accountable
- Effective monitoring
- Formal change management process
- Service level agreements
- Continuous improvement
- Strong business relationships
- Predictability
- Quality driven

Advanced

- Proactive
- Optimizing costs and quality
- Agile
- Fully automated
- Complete integration
- Enterprise-wide knowledge
- Planned innovations
- Change management fully implemented
- Strategic performance metrics

Polling Question

As you evaluate your organization's third-party relationship management process, where do you believe it falls on the maturity model?

a) Weak

b) Sustainable

c) Mature

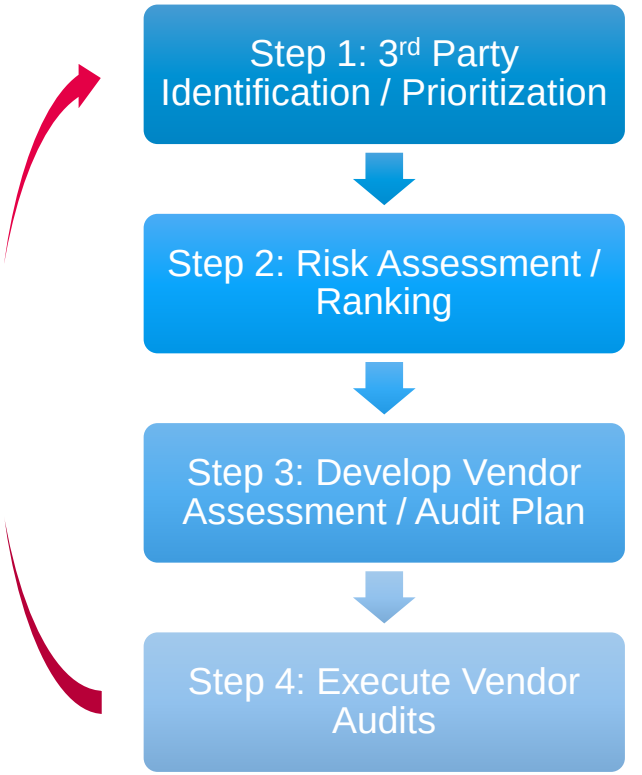
d) Integrated

e) Advanced

f) Unsure

RSM

Vendor Assessment - Methodology



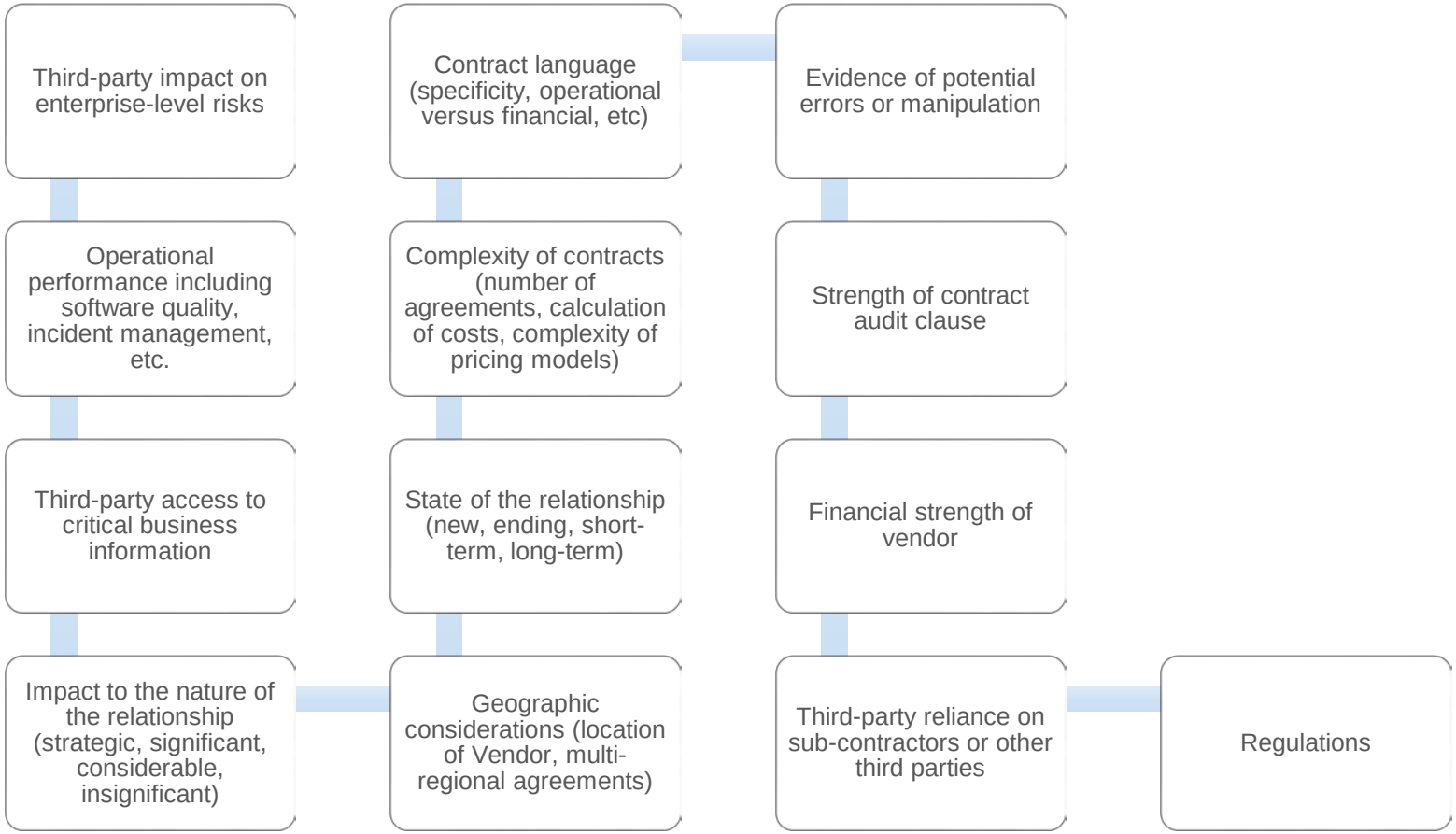
Continuous Monitoring

- Ensure completeness of your vendor / 3rd party population.
- Develop a risk assessment workflow which takes into consideration:
  - Operational Performance
  - Customer Service
  - Security (Information Privacy and Protection)
  - Regulatory Compliance
  - Personnel
  - Financial
    - Total spend analysis
    - Tax analysis
    - Self reporting accuracy
    - Other financial clauses (MFN, SLAs, etc.)
- The extent of procedures performed as a part of vendor audits should be tailored based upon risk rankings, stakeholder feedback, and the vendor's position on the TPRM Maturity Continuum.

RSM

Vendor Assessment - Factors for Prioritization

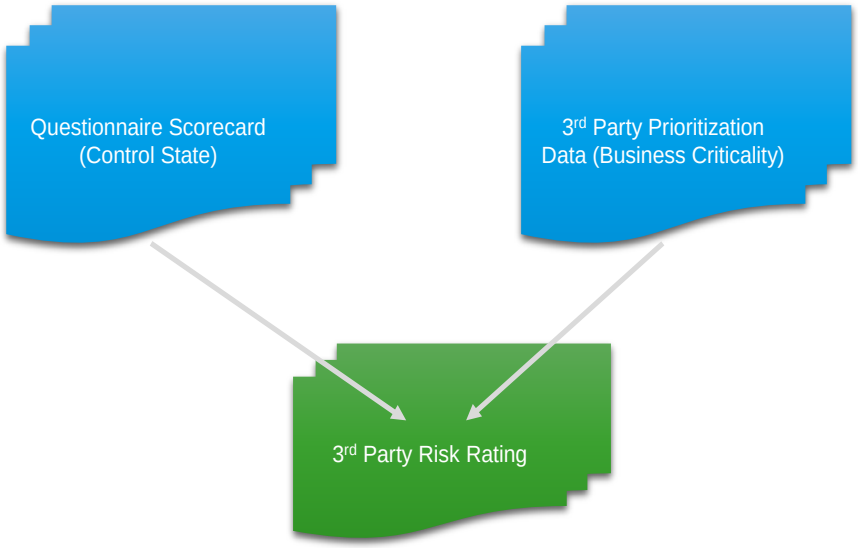
Third-party risk areas, and third parties themselves, can be prioritized based on factors such as:



Vendor Assessment - Risk Ranking

The goal of the third-party risk assessment workflow is to assess the level of risk third-party relationships present to your organization.

- The third-party criticality is determined from the Prioritization Data evaluation.
- The control state is determined from the questionnaire scorecards.
- These two data points contribute to the combined third-party risk rating, which drives the level of focus and attention the third-party needs to be given from a security perspective.

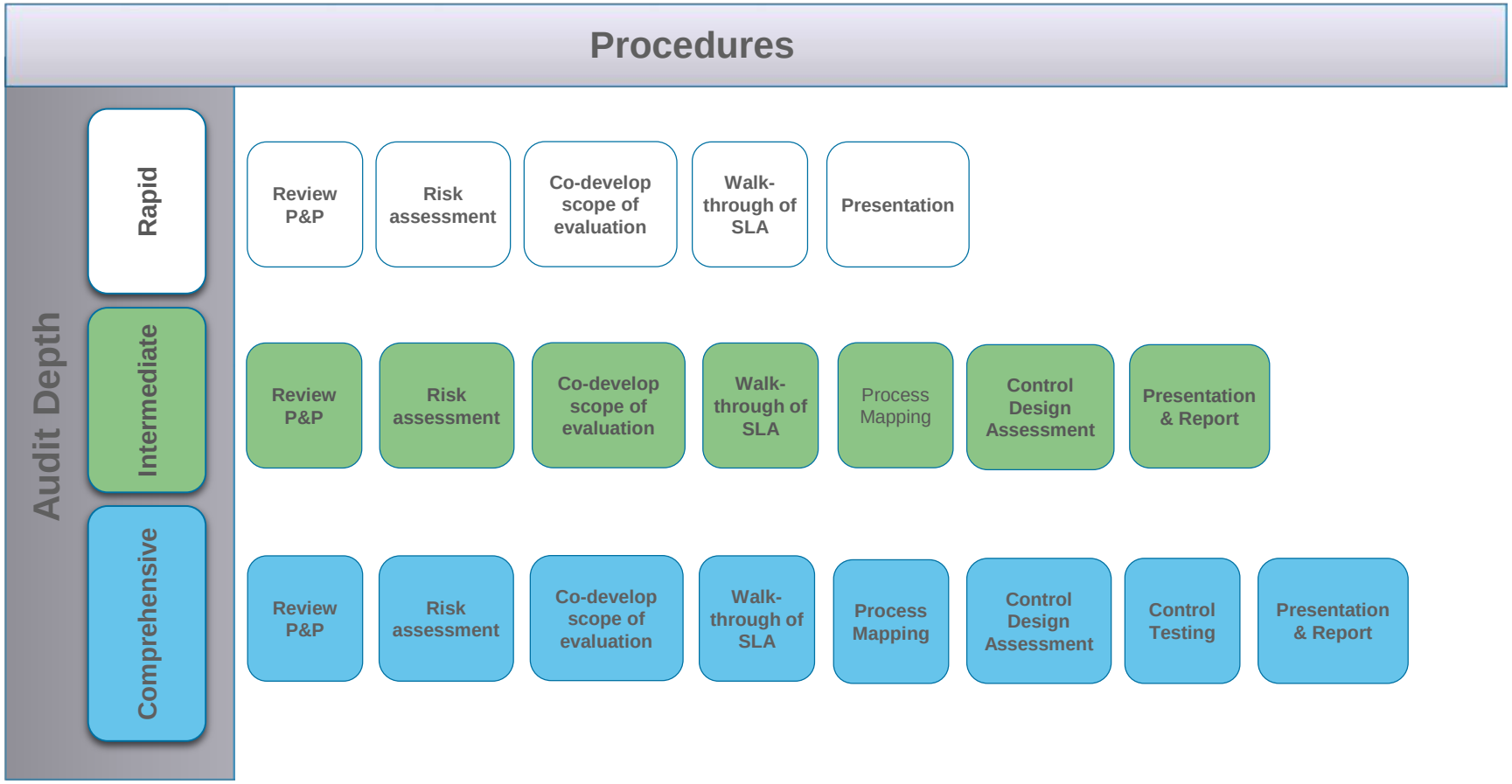


Control Score

	<50	50 -75	75<
3	Medium Risk	High Risk	High Risk
2	Low Risk	Medium Risk	High Risk
1	Low Risk	Low Risk	Medium Risk

RSM

Vendor Assessment – Approach



QUESTIONS AND ANSWERS?

RSM US LLP

7351 Office Park Place
Melbourne, FL 32940
321.751.6200

+1 800 274 3978
www.rsmus.com