Building Best Practices in Third Party Risk Management: Involving Procurement

A Shared Assessments White Paper

SHARED ASSESSMENTS

Abstract

Risk is agnostic. All organizations, regardless of size, maturity, or industry share key concerns in managing the growing complexities and scrutiny around risk in third party relationships. Each outsourced relationship presents its own unique set of risks with which organizations are challenged to effectively respond according to specific industry standards.

With the right tools and framework, the Procurement function can work closely, efficiently and effectively with all areas of an organization to help provide partners and regulators with a level of assurance that third parties are appropriately vetted and monitored throughout the life of the relationship. Procurement can also help facilitate a centralized process that is designed to mitigate many of the risks associated with these relationships and should therefore be seen as a critical function that organizations can leverage for more than just achieving cost savings.

Establishing a strong standard for risk management means including all stakeholders before a third party is brought on board. By consistently involving Procurement, Business Units, Risk Management and Legal in the third party on-boarding process, they can collectively establish a standard internal framework for handling third parties. This allows every department to remain advised of goals and objectives, so that they can each contribute the necessary elements to ensure that Request for Proposals (RFPs) and contract negotiations include elements of good risk management hygiene throughout the process

The focus of this white paper is to provide guidance on building such a framework, including Procurement as a critical stakeholder in Third Party Risk Management (TPRM) programs. Recommendations include the following:

1. Ensure the process is practical, sustainable and flexible, by applying four guiding principles in the development of a holistic framework of standards for vetting and onboarding third parties: consistency, objectivity, balance and management oversight.
2. Partner Business Units with Procurement to consolidate the use of third parties used for similar functions for economies of scale and risk mitigation.
3. Remain aware of potential concentration risk for third parties used for similar and critical functions.
4. Adopt methodologies that align with industry best practices, as well as regulatory requirements, which allows for the most effective risk ranking of a given third party's controls.
5. Assess controls during the RFP process and ongoing based on risk, execute favorable contracts and ensure a solid and comprehensive onboarding process.

An integrated approach consolidates third party onboarding processes, as risk ranking and negotiations take place in a consistent manner that aims to achieve common goals.

Issue Landscape

Whether or not an organization is regulated, the increasing use of third parties in the supply chain intensifies the risks to organizations at all levels. This is because the risk sphere includes every employee and business with which they have a relationship. Third and fourth party access to systems means that the controls protecting proprietary and other confidential information is exposed to downstream parties. TPRM programs should be designed to mitigate those risks that could negatively impact an organization. As an example, impacts from a third party's mishandling of sensitive information can have disastrous effects on an outsourcing organization, including operational issues that can cause significant loss of market share, customer confidence, reputation risks, regulatory fines and significant incident response costs.

However, many organizations fall short of this goal. For instance, the Office of the Comptroller of the Currency (OCC) reports five risk management issues they frequently observe when examining banks:

- Failing to properly assess, understand and document both costs and risk involved in outsourcing.
- Failing to perform adequate due diligence and monitoring of third parties.
- Engaging in third party relationships without formal or adequate contracts.
- Entering into third party contracts without assessing adequacy of third party controls.
- Entering into third party contracts that may incentivize a third party to take risks that are detrimental to the bank or its customers.[1]

1 *OCC BULLETIN 2013-29. Subject: Third-Party Relationships.* US Department of Treasury. Office of the Comptroller. October 30, 2013.

©2016 Shared Assessments Program. All rights reserved.

In addition, there are a myriad of regulatory requirements and industry standards affecting a wide range of verticals that are geared increasingly toward more effective third party risk management, including EU-US Privacy Shield (soon to be replaced by the General Data Protection Regulation or GDPR), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Payments Card Industry (PCI) Data Security Standards, Federal Acquisition Regulation (FAR) and Gramm-Leach-Bliley (GLB), to name just a few.

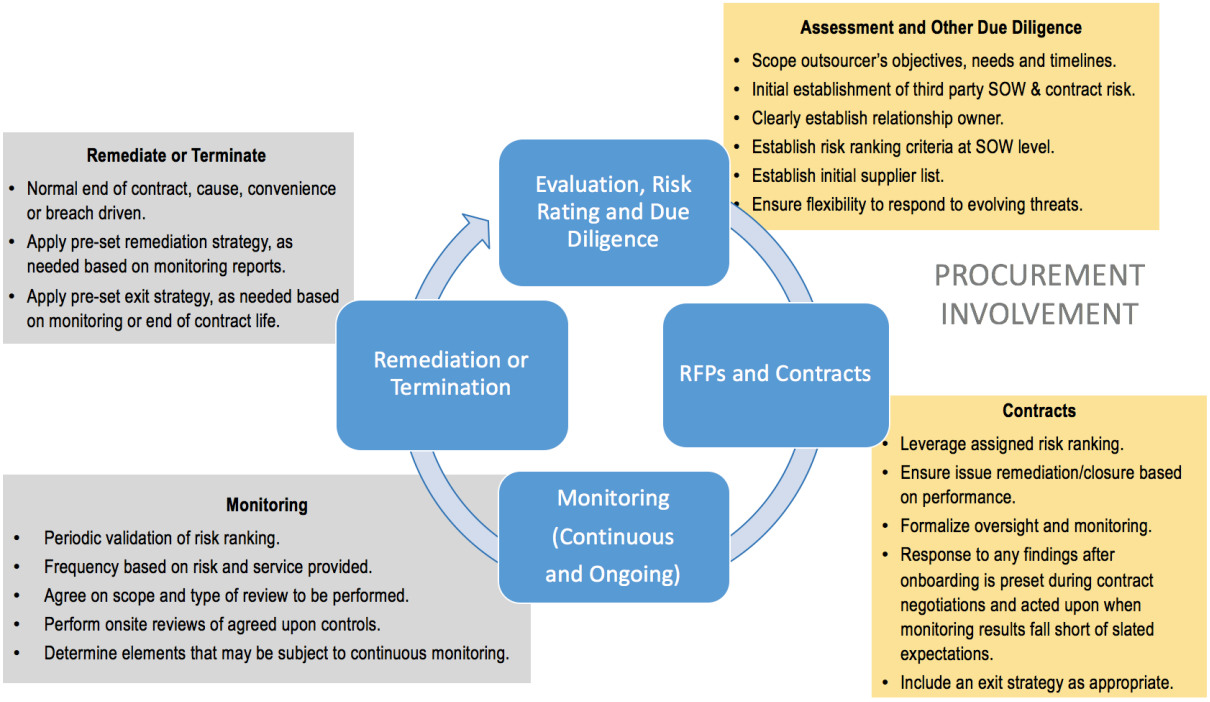
The Fundamentals

The siloed nature of business management activities, especially in larger organizations, can lead to inconsistent application of risk assessment standards and validation methodologies that can be ineffective at meeting the goals of such guidelines and standards. Currently, no industry-wide standards are applied for determining when in the onboarding process the acceptable level of risk for delivery of services is evaluated and managed. The initial tiering (or ranking) of a third party may take place during internal needs assessment, Request for Proposal (RFP), development or during other aspects of onboarding.

By applying a collaborative approach internally, an outsourcing organization can more readily and accurately identify and manage the risk created through third party relationships. Since robust risk management is heavily process-dependent, TPRM managers and other key leadership must be keenly focused on establishing effective processes that actively move their organizations' toward adoption of consistent, standardized and mature TPRM methodologies.

The following graphic shows the overall lifecycle for third party risk management processes. The areas for planning and onboarding a new third party, as they relate to risk management, are highlighted in yellow within the graphic.

The Third Party Relationship Lifecycle



©2016 Shared Assessments Program. All rights reserved.

Roles and Functions

The collective stakeholders for onboarding third parties are: (1) the Organization, which is the company seeking to partner with a third party; (2) the Business Unit, which is the department(s) or division(s) that require the use of external services; (3) Procurement (or Sourcing), which supplies: (a) the specialist and/or analyst who identifies potential third parties and, (b) the contracts manager who negotiates the third party relationship on behalf of the Business Unit and Organization and assists in ensuring due diligence is conducted; (4) the Third Party Risk Management (TPRM) Team, comprised of subject matter experts who conduct third party risk assessments on behalf of the Organization to identify information security, business continuity, disaster recovery, financial, internal controls, physical security and compliance risks to the Business Unit and/or the Organization; and (5) a Third Party Risk Committee, made up of a panel of cross-functional executives, whose objective is an ongoing assessment and evaluation of applicable third party engagements for overall risk and impact to the organization.

These roles and functions are defined in the context of each of the lifecycle tasks in Table 1 (at the end of this document). Organizations can use the guidelines in Table 1 to add dimension to their planning processes to optimize the critical role Procurement should play in managing third party risk. Understandably, not all organizations will have these roles/functions exactly as listed, and they may reside in business groups outside of the traditional Procurement function. Even so, it is critical that your organization identifies the right resources to ensure the appropriate amount of scrutiny is applied to third party relationships early in the TPRM lifecycle. Roles and functions should be clearly defined and communicated as part of a formal governance program.

Program Governance

According to the results of the 2016 Santa Fe Group/Shared Assessments study performed by the Ponemon Institute, *Tone at the Top and Third Party Risk Management*, no one department within organizations consistently owns TPRM. Compliance ranked highest at 23%, with Security Information at 17% and Procurement and Legal 15%. Yet respondents also reported that Compliance is the most likely department to take responsibility for risk-based assessments to be completed and all risks addressed (32%) and Lines of Business are reportedly responsible 27%, while Procurement took on this responsibility only 4% of the time – which is not consistent with assignment of ownership for that function. [2]

The critical workflow for any third party risk management program involves multiple processes of risk ranking, artifact gathering, control assessment, monitoring and mitigation of control deficiencies. Coordination between the business's service-level due diligence reviews and the risk assessment reviews is a must to avoid duplicate efforts from both the third party as well as your organization and will yield a much more comprehensive and holistic view of the relationship. Intervening in that process prior to fact gathering and assessment can proactively build mandates into assessment, ranking and controls processes that will improve an organization's overall risk posture. To implement a rigorous and standardized process of onboarding, communication and collaboration have become paramount in being successful in adequately assessing, identifying, reporting and resolving third party/engagement risks. Such communication should involve development of collaborative processes first, as policy will be more sustainable when it is based on solid structure.

A centralized governance model will provide the necessary support, guidance and controls needed to form the foundation of a successful program. As part of the governance structure, it is also good practice to have a group of senior level management, who are themselves subject matter experts in the risk industry, who meet on a regular basis to scope and review third party due diligence assessments, discuss third party concerns and trends and escalation policies assigned to risk assessment findings. To support this, it is extremely important to have a clear and communicated exception, escalation and incident management process as part of your overall program.

To be as efficient as possible in the assessment of third parties and their controls, Business Units should partner with Procurement to align sourcing and business delivery strategies and consolidate the use of third parties for economies of scale and risk mitigation, as well as to assess control weaknesses during the RFP process, execute favorable contracts and ensure a solid and comprehensive onboarding process.

2 *Tone at the Top and Third Party Risk Management*. Ponemon Institute and The Santa Fe Group, Shared Assessments Program. May 2016.

©2016 Shared Assessments Program. All rights reserved.

By working with all the stakeholder groups listed above in the Roles and Functions section, a governance function can be achieved that allows for a non-biased approach to risk review and creates layers of oversight in the event of needed escalation and exception requests during the third party relationship lifecycle. Organizations may consider multiple layers of oversight beyond what the relationship owner is responsible for. Business Units should work with Procurement to contemplate dual strategy for critical relationships, as well as leverage the subject matter expertise of individuals in the fields of Business Continuity, Disaster Recovery, Finance, Internal Controls, Legal, Information Security, Physical Security and Regulatory Compliance to ensure a thorough understanding of the potential risks associated with the relationship.

Centralizing Procurement

Creating such a centralized governance process using Procurement as the hub provides insight into all third party relationships and much needed control to the onboarding process and ongoing oversight of risky relationships. This is a critical aspect of building an effective third party oversight process, as it provides a single channel for all third party relationships. This single channel approach provides a governance check and balance process to maintain full adherence to policy and expectations by those with signatory authority throughout the negotiation and contracting phases. A central third party data repository should be maintained within Procurement with the assistance of Accounts Payable and other relevant stakeholders; this is something that is often absent within an organization due to the fact that third parties may structure their cost below what will trigger typical Procurement involvement in a third party engagement. As a dynamic operational process, it is important that Procurement meets regularly with each Business Unit to update the list of active relationships (i.e., Master Third Party Supplier List), confirm contact information, confirm the organization's most critical relationships and to ensure the scope and access to, or possession of, sensitive data within each relationship is accurate. The schedule and scope of risk assessment is heavily reliant on this information, so it must be refreshed routinely to support each organization's risk tolerance levels.

The risk oversight aspect of the Procurement program should take a holistic, risk-based approach and focus on the higher risk, or potentially highest risk, relationships. To help standardize an organization's processes so that they are consistent and repeatable, third party approvals can be set up that yield approval/denial options, such as: approved; approved with specified remediation required within a given timeline; not approved (denied); withdrawn by Procurement; or withdrawn by Business Unit.

Building Best Practices Involving Procurement

To integrate the third party oversight function into a Procurement program, stakeholders should focus on the following aspects of onboarding.

1. *Selection and Due Diligence Strategies:* Partnering Procurement early in the selection process with business relationship and other stakeholders:
    - Ensures a systematic approach to third party selection and oversight.
    - Provides the opportunity for Procurement to work with the other stakeholders to:
        - Help develop risk-based sourcing strategies that assist in the selection of third parties.
        - Identify potential third parties who provide the desired service/product.
        - Develop and implement a Request for Proposal (RFP) or Request for Information (RFI) process that includes all relevant business requirements and control areas.
        - Provide analysis of the RFP/RFI responses and/or facilitate a deeper due diligence by leveraging subject matter experts in the appropriate field(s).
        - Ensure that requirements for critical processes are clearly communicated.
    - Realizes strategic benefits that include negotiation leverage.
    - Ensures that the onboarding process moves as efficiently as possible.

©2016 Shared Assessments Program. All rights reserved.

- Coordinates internal requests to the third party for similar artifacts for different Business Units.
- Provides the opportunity for designing an RFP template that aligns with control requirements.
- Establishes a central repository within the organization for third party information with the results of RFP activity that includes: which third parties have access to sensitive data; active and anticipated third parties; whether or not a third party is approved or declined and why. This time-saving measure will create the ability to track third parties in a living document (i.e., Master Third Party Supplier list) that is continually updated in partnership with Accounts Payable on a regular cycle. the opportunity for designing an RFP template that aligns with control requirements.

2. *Contract Terms and Conditions*: Procurement should be part of the contract review for all third party agreements, including Master Agreements, Statements of Work (SOW) and Service Level Agreements (SLAs). This involvement includes:
   - Develop and implement an unambiguous "Data Security Exhibit" that articulates requirements a third party must meet based on that particular relationship's unique risk factors
   - Ensuring that appropriate clauses are included in agreements for critical relationships and for third parties who will have access to non-public information, such as: putting a process in place to periodically perform a contract audit for strategic suppliers; making sure to include incident management parameters and creating corrective action/remediation plans that include escalation and exception processes; and requiring a formal business resiliency program is in place.
   - Procurement can consistently include terms that make the third party contractually obligated to comply with the outsourcer's due diligence and mitigation for any areas of risk identified during the due diligence process (e.g., assessment techniques, increased insurance amounts, etc.).
   - Identifying and aligning impactful qualitative and quantitative metrics to measure Key Performance Indicators (KPIs) and SLAs that tie directly into department and/or organization goals.
   - Executing agreements and managing contract workflow.
   - Ongoing assistance in third party management plans, guidelines, scorecards and routine meetings, and filling any need to tap into external resources for due diligence reviews.
   - Timely notification to the Business Unit of upcoming contract renewals.
   - Consider an "Exception with a Commitment" to move the organization's third party population incrementally into full compliance with risk rating requirements. This should be tracked as ongoing remediation activity until this is achieved across the third party population.
   - Employ "complete, share with many" documents and artifacts with the third party population to drive ongoing efficiencies and use of common processes and procedures.
3. *Ongoing Risk Management and Oversight:* Throughout the life of the relationship, Procurement should be seen as an ally and a resource to the Business Unit, which can
   - Assist in the ongoing review of service level agreements, performance goals, risk considerations, incident tracking and management, communication protocols and carrying out exit strategies:
   - Work closely with the relationship owners of each third party relationship, as well as internal subject matter experts, in the review of high risk relationships, as defined by your organization.
   - Help maintain appropriate TPRM tools enterprise wide, leveraging risk management software to streamline the process and minimize the opportunity for human error that can compromise the integrity of information and reporting and make unnecessary redundancies and intercompany synergies more apparent. Automation can also help with scaling the process; it will keep the process repeatable and auditable.

©2016 Shared Assessments Program. All rights reserved.

A holistic, risk-based approach to third party oversight is the recommended method, in which all stakeholders work together, including Procurement, to manage supplier performance, set metrics, measure and follow-up on non-performance. As it is not practical to look at every third party relationship in minute detail, Procurement can serve as a centralized mechanism for establishing and adhering to a solid pre-assessment process. In this way, only the necessary third parties are vetted through specialized due diligence, allowing due diligence to be right-sized by having processes that are applied based on the inherent risks and complexity of the relationship. Such an approach also benefits the Business Unit in not having to develop a high level of expertise in areas where they may only become involved one or two times a year.

Benefits

Business lines within a given organization share many common service needs and risk profile concerns. Tangible gains in risk posture and TPRM efficiency can be seen over the long-term by applying a standardized governance model that uses proven tools and centers around Procurement from the outset of a third party relationship. Procurement has a body of knowledge that can be leveraged when brought to the table.

Creating such a centralized governance process using Procurement as the hub for third party selection provides key benefits:

- All third party relationships start and end with Procurement.
- Essential control and comprehensive, right-sized oversight.
- Process effectiveness.
  - Stakeholders are engaged at key, risk-based process points.
  - Third party management is improved, even beyond risk concerns.
  - A central data repository is created with a specific owner (Procurement).
  - A consistent repeatable, robust process is established.

The overarching benefits of this systematic approach to third party selection and oversight include:

- More robust protection for the outsourcer, through increased rigor.
- Greater assurance for due diligence, through standardization.
- Greater efficiency, through economy of scale achieved by consolidating third party risk management processes.
- An overall stronger central risk function capacity.

Additionally, effective contract negotiations tend to create better supplier segmentation, allowing businesses to identify and track their top suppliers and – as a result – better manage risk.

Conclusion and Next Steps

All organizations face an ecosystem which demands an increasingly more diligent and efficient approach in third party lifecycle management processes in order to remain sustainable. Adopting an industry-wide, standardized approach that involves Procurement in the onboarding process can reduce risk management burdens for both outsourcers and third parties. This collaborative approach that involves all stakeholders from the outset gives programs the power to leverage processes and tools from internal business partners, utilize industry standard questionnaires and practices (Shared Assessments) and plug into other industry resources (paid and free). In turn, organizations employing this internally-collaborative strategy can drive down overall costs and streamline processes, while incorporating best practices, gaining greater agility in risk reduction and improving communications with business partners.

In summary, a mature TPRM program will benefit the organization by building an effective Procurement framework, applying four guiding principles:

- *Consistency*: Develop a framework and institute standard templates for vetting your third parties. Move toward an automated process to drive consistency across your organization.
- *Objectivity*: Create a process that is free from bias to avoid inherent conflicts of interest.

©2016 Shared Assessments Program. All rights reserved.

- *Balance:* Develop a risk-based approach to due diligence that allocates resources appropriate to the risk of each given relationship to ensure the process is practical, sustainable and defendable.
- *Management Oversight*: Early involvement of Procurement, alongside Business Unit owners and management that will conduct oversight, is key to risk management.

Creating a program that is designed to mitigate the risks associated with third party relationships is not a simple feat. Procurement should work closely with the business owners of each relationship as well as with the appropriate group of subject matter experts to review potentially new relationships prior to signing a contract, as well as working with high risk third parties throughout the life of the relationships.

Such collaborative involvement fosters communication throughout the organization by keeping company leadership apprised of significant risks in addition to holding regular on-going performance based meetings with both the business and their third party relationships and include escalation, exception and incident management processes as part of the overall program.

About the Shared Assessments Program

The Shared Assessments Program is the trusted source in third party risk management, with resources to effectively manage the critical components of the vendor risk management lifecycle that are: creating efficiencies and lowering costs for all participants; kept current with regulations, industry standards and guidelines and the current threat environment; and adopted globally across a broad range of industries both by service providers and their customers. Shared Assessments membership and use of the Shared Assessments Program Tools: Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means of conducting rigorous assessments of controls for IT and data security, privacy and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Thank You to Our Contributors

This paper is part of a series of papers on best practices in third party risk management. We'd like to thank the Shared Assessments Best Practices Group volunteer members who contributed so generously to this paper:

- **Christina Howlett-Perez**, Procurement Manager, Wellington Management Company, LLP
- **Emily Irving,** Assistant Vice President, Vendor Risk and Oversight Manager, Wellington Management Company, LLP
- **Mitchell Kavalsky**, Program Lead, Security Policy and Governance, Sungard Availability Services
- **Shawn Malone**, Vice President-Business Compliance, Radian Group Inc.
- **Anindity Roy,** Senior Manager, Enterprise Risk Consulting, Genpact USA
- **Peter Tannish,** Information Security, SBFE, LLC

We would also like to acknowledge The Santa Fe Group staff who supported this effort:

- **Tom Garrubba,** Senior Director, The Santa Fe Group, Shared Assessments Program
- **Robert Jones,** Senior Advisor, The Santa Fe Group, Shared Assessments Program
- **Charlie Miller**, Senior Vice President, The Santa Fe Group, Shared Assessments Program
- **Marya Roddis**, Vice President of Communications, The Santa Fe Group, Shared Assessments Program

Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

©2016 Shared Assessments Program. All rights reserved.

SHARED ASSESSMENTS

Third Party Risk Management – Involving Procurement Guideline Tool

Planning and Communications Roles and Responsibilities *

Third Party Selection: Evaluation, Risk Rating and Other Due Diligence	**Potential Process Owner**	**Additional Stakeholders**
Set internal objectives: • Need and scope of services (SOW). • Set timelines. • Due diligence requirements defined.	Business Unit	TPRM Team, Procurement, TPRM Committee, Business Continuity, Finance
Set internal budget: • Cost analysis. • Agreement among stakeholders.	Business Unit	Procurement, Finance, Accounting
Market (service/product) analysis: • Identify known opportunities/risks/alternatives. • Report to stakeholders.	Procurement	Business Unit(s), TPRM Committee
Establish initial risk ranking criteria for responses: • Simple, clear, consistent. • Applied at the SOW level. • Leverage industry standards. • Determine which control assessments areas will be included (security, information, personnel, site, business continuity and resiliency, regulatory, etc.).	Procurement	Business Continuity, Disaster Recovery, Internal Controls, Information Security, Physical Security, Legal, Regulatory Compliance, TPRM Team
Develop initial supplier list: • New/existing. • From Request for Proposal responses, sole source or renewals. • Initial risk ranking for potential suppliers.	Procurement	Business Unit(s), TPRM Team
Contracts: RFP & Contracting Process for Onboarding		
RFP and negotiation strategy development: • Include communication planning for launch.	Procurement	Business Continuity, Disaster Recovery, Internal Controls, Information Security, Physical Security, Legal, Regulatory Compliance, TPRM Committee, TPRM Team
RFP drafting and release: • Initial statement of SLA and KPI development & monitoring expectations/cycles. • Include questionnaires to allow risk ranking. • Capture required documentation.	Procurement	Regulatory Compliance, Legal

©2016 Shared Assessments Program. All rights reserved.

Negotiations and deal approval: • Risk ranking of responsive third parties based on pre-established criteria and questionnaires received with RFP responses. • Finalize expectations through SLAs. ▪ Contract Legal-approved clauses (right to audit, information and physical security, business/recovery plans, fourth parties, encryption requirements, termination/exit provisions, etc.). ▪ Due diligence (background checks, authorized signers, business/resiliency planning reviewed, formalize contingency planning, specialized services, legal, etc.). ▪ Exceptions and approval (generally signed by the Business Unit).	Procurement	Regulatory Compliance, TPRM Committee, Legal, Business Unit(s)
Launch third party.	Business Unit	Accounting, TPRM Team
Monitoring , Remediation and Termination: Third Party Management after Onboarding		
Implement supplier management plan, guidelines, and scorecards: • Leverage assigned risk ranking and prior reviews. • Based on negotiated monitoring/reporting SLAs and KPIs. • Onsite inspections.	Procurement	Compliance, TPRM Team, Business Unit
Ongoing risk assessment monitoring and oversight: • Control testing. • Risk assessment reporting. • Senior management reporting. • Performance/management review. • Software/license compliance. • Issue remediation/closure (as needed).	TPRM Team	Compliance, TPRM Team, Business Unit
Termination: • Follow pre-determined exit strategy. • Normal , cause, convenience or breach. • Asset return and/or confirmation of destruction of confidential data.	Business Unit	Procurement, Accounting, Technology Services, TPRM Team, Compliance, Legal

* This guide can help your organization identify the right resources in your planning and implementation processes, in order to apply an appropriate amount of scrutiny to third party relationships early in the TPRM lifecycle. Each organization must evaluate this process from its own standpoint, based on their own model (e.g., centralized versus decentralized) and the players appropriate to their individual organization's needs.

©2016 Shared Assessments Program. All rights reserved.