SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

BUILDING BEST PRACTICES BRIEFING PAPER

USING TPRM BEST PRACTICES TO IMPROVE M&A OUTCOMES

TABLE OF CONTENTS

EXECUTIVE SUMMARY 3
Figure 1: M&A Five Phases and Descriptions 4
M&A ISSUE LANDSCAPE – THE CHALLENGE 5
Key Definitions 5
Raising the Bar for M&A Due Diligence – Improving Outcomes 6
EMERGING BEST PRACTICES – THE SOLUTION: LEVERAGING TPRM TECHNIQUES 7
M&A from Various Perspectives 7
ACQUIRERS 7
TARGETS 8
MERGER OF EQUALS 8
M&A Due Diligence – Gaining Essential Insight 8
TPRM BEST PRACTICE TOOLS AND TECHNIQUES PROMOTE EFFICIENCIES 8
ASSIGNING APPROPRIATE RESOURCES 9
LEVERAGING TPRM BEST PRACTICES & TECHNIQUES 9
Imparting Improved Structure to M&A Due Diligence 10
Brokered Assessment Repositories and Assurance Portals 10
Initial Assessments and Standardized Questionnaires 10
Onsite and Virtual Assessments 10
Use of Auction Rooms 10
LEVERAGING PRACTICES BY PHASE OF M&A 11
Figure 2: M&A Phases and Related TPRM Best Practices 11
Pre-Selection (Strategic Planning) 11
Selection (Target Phase) 11
Pre-Signing (Negotiation) 12
Figure 3: Integration Planning 12
Acquisition (Post-Signing/Pre-Closing) 13
Post-Closing (Integration) 13
BENEFITS AND CONCLUSIONS 14
APPENDICES – GUIDELINE TOOLS FOR PRACTITIONERS 15
Appendix 1: Due Diligence Checklist 15
Figure 4: Shared Assessments Program 18 Risk Domains 15
Appendix 2: Due Diligence Outcome Documentation 18
Acknowledgments 22
ABOUT THE SHARED ASSESSMENTS PROGRAM 22

SFG | SHARED ASSESSMENTS

BUILDING BEST PRACTICES:

Using TPRM Best Practices and Tools to Inform M&A Transactions

Executive Summary

The need has grown in most Merger & Acquisition (M&A) environments for enhanced, risk-related due diligence. Improved risk governance is essential to respond to the challenge. Third Party Risk Management (TPRM) processes are ideally suited to enhancing due diligence throughout the M&A process.

The Challenge

The need for improved M&A due diligence practices is becoming increasingly clear.

- Significant loss in value post-acquisition in several high profile instances has resulted from insufficient due diligence into risk practices. The lack of robust due diligence leads to a failure to identify and/or respond to predictable and significant impacts prior to the close of M&A transactions.[i]
- Regulators are placing emphasis on risk-related M&A due diligence. As recently as February 2020, the European Data Protection Board (EDPB) emphasized the importance of due diligence in mergers and the privacy implications and data protection impacts of mergers.[ii]

An Innovative Solution

Incorporating proven TPRM practices into M&A activities can provide greater visibility into issues across all phases of M&A due diligence. TPRM best practices can be applied broadly to due diligence for any transaction, not just to those risk areas that are typically associated with outsourcing to Third Parties. TPRM is agile enough for M&A's quick turnaround timelines. The skilled resources required to apply TPRM processes and tools to M&A settings often already exist within organizations under the umbrella of vendor risk management.

This TPRM-focused M&A guide:

- outlines TPRM best practices that can help substantially lower risks in M&A settings;
- discusses both acquirer and target viewpoints; and
- provides how-to guidance for integrating TPRM policies, process and technologies into M&A settings.

Gaining Essential Insight

This paper and guideline tools take into account that companies engaged in M&A activities may be guided by a wide range of concerns; all of which require early insight into material and other adverse change risks that might affect the business case for the deal.

By applying the TPRM lens, tools and techniques to M&A discovery processes, a degree of incremental risk can be examined that may otherwise be overlooked, identifying a wider range of risks deeper in the supply chain than is typically achieved in M&A due diligence.

Using TPRM Best Practices and Tools to Inform M&A Transactions

This approach yields:

- **Efficiency:** The information gained through adopting this approach can be expected to improve the efficiency of M&A due diligence, inclusive of continuous monitoring.
- **Transparency:** This deeper insight can also provide greater transparency throughout the deal. For instance, an improved understanding of risks can be gained about a target company's geo-footprint, financial standing, use and connections to Nth Parties and other essential intelligence. This risk-focused intelligence in turn better informs an early understanding of the consolidated deal risk profile, which can then be examined in greater depth as the deal progresses.
- **Effectiveness:** By incorporating TPRM best practices into integration planning, potential issues can be revealed early in the deal, exposing latent integration issues and provides the basis for a risk-based, and prioritized deal action plan that can be more effectively executed.

The Phases of M&A – Terminology and Tasks

As the phases of M&A may be defined differently in various organizations, for the purposes of this paper and our discussion, we have defined five distinct transaction phases, as described in Figure 1.

Figure 1: M&A Five Phases and Descriptions

Benefits and Conclusions

Because TPRM tools and oversight processes provide such a powerful model for many aspects of M&A due diligence, the risks and opportunities associated with any transaction will come into significantly sharper focus. Risks examined can fall across any functional area of an organization, including the acquiring line of business, business operations, information/cyber security, technology, human resources, physical security, business continuity, Third Party management and oversight, negative news, etc.

Throughout the M&A process, all significant risks, including cyber risks, should be brought to the attention of acquirer C-suite management and boards of directors. The board can then make informed decisions and re-examine the organization's risk appetite to ensure that known impacts related to the acquisition are taken into account during the deal. Using this best practice approach to due diligence provides defensible evidence in the event that something comes to light after acquisition that is of negative impact.

M&A ISSUE LANDSCAPE – THE CHALLENGE

While every company is different in its M&A strategy and every circumstance is different, across the spectrum, TPRM due diligence processes can:

- provide valuable insight into identifying and managing a broad range of risks; and
- apply proven, robust practices that can foster more effective arm's length working relationships between both parties in a transaction.

M&A deal due diligence should include:

1) **Pre-Selection:** Scope and review a range of deal structures, the seller environment (physical, operations, technology, governance, risk management) and identify appropriate risk domains for due diligence.
2) **Selection:** Initial screening and monitoring through publicly available information. At later stages in this phase the acquirer may request additional, filtered, relevant-to-deal documentation from the target.
3) **Pre-Signing:** Determine (typically with legal counsel) what documentation is required and how that documentation will be exchanged and made available to the counterparty (e.g., through a repository or a data room). Review documentation, conduct interviews, begin to create debriefing (aka "out brief") documents for use in later stages. Rate parties against pre-determined criteria that are based on the acquirer's risk appetite. Examine findings, analyze and identify any red flags. Set out remediation pathways. If any red flags are not remediable, consider whether to kill or otherwise modify the deal early. Formalize integration plans – including development of Transition Services Agreements (TSAs), improving control requirements, planning incremental training, etc.
4) **Acquisition (Post-Signing/Pre-Closing):** Review any remaining issues; conduct agreed upon ongoing/continuous monitoring. Document an agreed upon integration and monitoring plans and reflect those plans in contract terms.
5) **Post-Closing:** Conduct ongoing monitoring, implement TSAs, trainings, etc. Evaluate integration and operations during and after transition.

Key Definitions

Business Continuity and Resilience while not synonymous, these terms are complementary in that they both revolve around the assurance that an organization's business functions will either continue to operate despite serious incidents or natural disasters, or may otherwise recover within a pre-determined period of time.

Legal Day One (LDO) is a term that conveys the priority of what deal decisions and controls need to be in place on the first day post-closure. Typically these items include personnel, change of control and corporate governance obligations.

Merger of Equals is a term often utilized by management when similarly sized companies consolidate. While so-called "merger of equals" are fewer in number, they may raise additional considerations for risk management hygiene and culture. Often, in fact, there is a junior or senior partner, but in some industries special care may be taken to avoid such a perception. Social issues may become more important when two similar parties merge, and executive management may find it more difficult to create an appropriate integrated risk culture and may face more friction in the integration process after a transaction closes.

Onboarding is the process of integrating a new Third Party into an organization. Onboarding occurs after initial due diligence has been completed, the Third Party has been selected and a contract has been signed.

Partners are the two primary actors in the deal – the acquirer and the target.

Red Flags are deal-related issues that when identified may have significant negative impact on the M&A and could put the deal at risk or increase remediation and/or integration expenses.

Risk Appetite is the level and type of risk an organization will accept in order to pursue its strategic measurable objectives. A Risk Appetite Statement is the documented definition of the organization's risk appetite.

Risk Capacity is the highest level of risk that an organization is safely able to take on in pursuit if its goals.

Risk Profile is a quantitative analysis of all of the known risks an organization is facing at any point in time.

Target is the unified term used for the company being acquired. Targets of mergers and acquisitions are, in effect, Third Parties to the acquirer.

Raising the Bar for M&A Due Diligence – Improving Outcomes

M&A due diligence practices around M&A have not kept pace with the rapid increase across all industries in the use of outsourcing. TPRM is an important, yet often overlooked segment of M&A due diligence, and can have a significant impact on post-merger outcomes for an acquiring organization. The same techniques that are used to determine the hygiene of Third Parties can be used effectively to understand the operational risk management maturity of target organizations, However, the use of TPRM techniques have farther reaching implications for M&A due diligence which have the potential to improve deal outcomes.

Standard TPRM processes can help uncover risks beyond those associated with third parties. For instance, Third Party hygiene that increases risks beyond the acquirer's risk appetite has the potential to increase financial and reputational costs for the acquirer after closing.

The impacts of inadequate M&A due diligence are known to be serious for an acquirers. Examples of significant issues that have negatively impacted M&A deals, include:

- **Prior Seller data loss events** unknown at the time of signing or close (Verizon/Yahoo – Cybertalk.org, 2018, PayPal/TIO Networks – Cnet news, 2018, Marriott/Starwood Hotels – engadget.com, 2018).
- **Malicious code introduced through the supply chain**, not previously known by the target, passed on to the acquirer (Avast/Piriform – wired.com, 2018).
- **Operational impacts to new services and customers** now associated with the acquiror's brand (FedEx/Bongo – cybertalk.org, 2018).
- **Possible state-sponsored attempts to infiltrate the supply chain** through hardware (Super Micro – Bloomberg, 2018).
- **Timing of inherited liability** for post-close breach disclosures or other significant unmitigated risks that may be known yet ignored (Dow/Union Carbide, Chevron – theguardian, 2019).

Essential points where early assessment may identify red flags include:

- **Target management shows reluctance to assist in discovery.**
- **Public records show negative or contradictory information.**
- **Evidence of inappropriate level of (or incomplete) due diligence risk culture**, such as:
  - Target proves to have little risk management process or documentation using only limited assessment and monitoring in place of a wider, pre-designed/pre-approved due diligence process.
  - Target's information is contradictory, inaccessible, poorly organized, not automated, not provided in a timely manner or wholly absent.
- **Undisclosed or unassessed Nth Party supply chain risks** may require special examination, including service providers, suppliers, distributors, agents, unions, affiliates or joint ventures; distribution channels (shipping, retail, etc.); and previously unused technologies under consideration or technologies that introduce unique risks.
- **Lack of a** governance culture **or internal controls.** Goals, practices and processes can all differ across partner's cultures. To reduce significant social issues that may make the deal untenable, an understanding must be reached regarding which people, technology and processes will be continued in the combined company. An acceptable risk appetite for targets is set and documented by the acquirer, which the target's culture must match. Of note, acquisitions that cross national borders can involve significant complexities to unite corporate governance.
- **Offshore Vendor Relationships.** Target may be reliant on Nth Party providers or supply chain in offshore locations which may add both risk and complexity to integration planning.
- **Possible indicators of the need for enhanced due diligence** include short business tenure; pending legal action for key staff, conflicts of interest, or other telling information; financial crime concerns; and new products or new lines of business. In high risk industries, such as pharmaceuticals and financial services, unique and thorough due diligence attention is required, including compliance with "Know Your Customer" KYC laws (Internal Revenue Service Revenue Procedure 2000-12; US Department of Treasury. 2020).

In public-private mergers, certain private company processes must be altered in response to regulations governing publicly-held companies. Any financial reporting, accounting, compliance and ethics obligations will apply to the acquired company governance at the time of deal closure. That requirement mandates that related controls are in place on Legal Day One and must be documented,

communicated and executed in accordance with agreed upon plans. This requirement can reshape the order of execution for M&A plan due diligence processes and other integration priorities.

Areas of risk that deserve examination during due diligence include: Environmental, Social, and Governance (ESG), i.e., ethical sourcing issues, such as human rights and labor, governance formal oversight around environmental issues, whistleblower programs; as well as business resilience, legal risks, ethics and reputation and anti-corruption policies and processes, covered by ISO, FFIEC, GDPR, EBA, PCI-DSS, United Nations Global Compact, state and international privacy requirements, and other relevant standards and regulations.

Any issues discovered during due diligence must, of course, be addressed. To encourage transparency, acquirers can build in contract terms that take into account any Post-Closing 'out of scope' discovery issues that may have a direct, quantifiable, retroactive effect on the sale price or earnout provisions. Obviously, in a best case scenario, issues identified should be mitigated prior to deal close and assured contractually in Conditions of Closing. There may also be instances where principals may need to divest if shared ownership presents perceived conflict.

EMERGING BEST PRACTICES – THE SOLUTION: LEVERAGING TPRM TECHNIQUES

A major requirement for improving M&A outcomes is putting in place the right risk resources environment and bringing the right people to the table early in the deal. This requires that teams with pertinent risk management expertise should be assembled to enable them to play an appropriate guiding role in the M&A process. Assignments should be documented detailing who will be responsible and accountable for specific tasks and for the due diligence planning and execution, including setting and meeting key milestones, as well as sharing gathered information in a timely and appropriate manner.

Individuals included in those early discussions should also be informed about the confidentiality of and rules for sharing information in order to avoid insider trading, conflicts of interest or other regulatory hazards. Monitoring should be put in place for an "in-the-know list" of stakeholders that have access to non-public information during the course of the deal. Further attention to internal controls is vital since embezzlers and other economic criminals exploit the often rampant confusion that can occur during the integration process.

M&A from Various Perspectives

The Guideline Tools for Practitioners provided in the appendices of this paper gives acquirer and target perspectives. Best practices for each party, in summary, are as follows.

ACQUIRERS

Acquirers should set key risk-related criteria for evaluating potential targets. The acquirer should understand and document consortiums, joint ventures, growth/expansion plans, existing contractual or other significant responsibilities and risks that may exist with both the target and its Nth Party supply chain. *It is not uncommon for acquirers to walk away from transactions where risks appear to be excessive.*

Acquirers should be clear about what types of due diligence information will be needed from target companies and how and by whom it will be handled. For example:

- Acquirers should be prepared with a documented plan, sufficient personnel and the right processes and technology to manage the incoming information within deal timeline constraints.
- TPRM tools and domains should be used to systematically evaluate the target can be help in comprehensively identifying any issues prior to signing the deal.
- It is important that acquirers define and communicate expectations on how cyber security and security incident reporting issues are to be handled and reported.
- Acquirers should allocate resources according to the risk posed by a target (as well as a target's supply chain) and be clear about which function owns risks, and then build risk ownership into the workflow, documentation and processes. *Where appropriate internal resources are unavailable, it is best practice for acquirers to seek outside expertise.*
- Verification of findings should be undertaken prior to closing.

Because entering new markets may expose acquiring parties to new risks (including unanticipated emerging regulations driving expanded compliance obligations as well as new legal issues), it is important that acquirers be prepared to resolve a wider range of issues than they have previously faced internally prior to deal closure. Acquirers should identify and document newly required process management roles and address the range of issues that have been identified as requiring remediation (either by the

target prior to close, or by the acquirer prior to or promptly following closure). Escalation processes should be put into place that will be triggered when critical, predetermined deal breaker issues arise with either partner.

TARGETS
When a firm seeks a buyer, the organization should be aware of the picture it presents to the market in order to maximize its attractiveness to potential partners. A company may be in the position to be a target for M&A for a variety of reasons including financial, capacity or change in leadership due to attrition. Reluctant sellers may have faced financial challenges, yet retain strong interest in the business succeeding in the long term and therefore may remain strong partners. Willing sellers may include startups and other companies that require a larger platform to be successful over the long term.

Regardless of their position, sellers can best position their company in the market by anticipating acquirer needs and concerns. Potential targets should expect and be prepared to respond to quick timelines during negotiations and signing.

Transparency is important when sharing known issues or concerns; the focus shifts to risk mitigation post close, but with shared accountability. Proactive self-assessments, such as Risk Control Self-Assessment (RCSA), and independent verification of those assessments can provide valuable governance information. TPRM tools and processes can be effective in enabling the target to self-identify and mitigate issues prior to or during the acquirer's due diligence process. Small company targets may want to have themselves independently reviewed – if they are positioned to do so.

Targets should:

- prepare data ahead of time (prepare sanitized network diagrams, data flow diagrams including data that may flow to Nth Parties, RCSA, etc.);
- secure documentation on supplier and other Nth Party assessment and contracts, leasing and rights (IP) information; and
- remediate compliance or other serious issues ahead of M&A offering.

Targets also need to be prepared for due diligence as an ongoing process Post-Closing, as the process simply shifts into the next phase and may require ongoing participation and additional artifacts.

MERGER OF EQUALS
A mergers of equals M&A setting introduces unique risk exposure that could create issues. Social and cultural issues require quick integration of risk management structures and common TPRM processes to reduce the friction involved in merger of equals settings. Executive managements and the boards of directors should take special care to define and reinforce risk culture expectations.

Regardless of the posture of the parties (acquirer, target, merger of equals), roles and responsibilities of senior managers in the consolidated entity should be made clear and announced at or just after deal closing. Employees of either company who perceive themselves at risk of their job when the deal closes may themselves present a heightened risk of intellectual property or other loss. Since that possibility exists, the need for robust Data Loss Protection (DLP) becomes even more important, including cyber and other security training, criminal history checks and formal acceptance of code of ethics statements. Use of employee retention agreements for key employees is a tool used to reduce, but not eliminate, this risk.

M&A Due Diligence – Gaining Essential Insight

TPRM practices can be leveraged to facilitate both parties' due diligence efforts. TPRM tools are designed to examine risks across the threat landscape, including cyber, security policies, physical and environmental security, business resilience and operations management. Adapting this model to M&A settings can therefore enhance assessments across the spectrum (e.g., application security, network vulnerabilities, patching cadence, obsolete , weaknesses in access management, data loss prevention). Using this best practice approach to due diligence provides defensible evidence in the event that something comes to light after acquisition that is of negative impact.

TPRM BEST PRACTICE TOOLS AND TECHNIQUES PROMOTE EFFICIENCIES
While M&A practices differ from organization to organization, TPRM best practices are proving successful as a process model in the M&A arena. Key TPRM practices in M&A settings include:

- **Assigning appropriate resources** that include experienced personnel with the relevant skills.
- **Standardizing materials** (assessment and field documentation templates, contract clause templates and expectations around risk domain controls and audit rights, etc.).
- **Utilizing risk-tiering** to assure an appropriate level of due diligence for both basic and comprehensive reviews.
- **Automating processes** to provide rapid response assessment and analysis.
- **Providing assurance to key customer relationships.** Organizations may have specific customer contractual notification provisions regarding M&A that must be observed.

- **Establishing a "Trust, but Verify" relationship between the partners.** Transparency is good for both parties in the long run – surprises may cause disruptions that work to the detriment of both.

ASSIGNING APPROPRIATE RESOURCES

A rapid response and analysis process should be put in place to deal with discovered risks. Senior staff, business units and other functions such as finance, legal, procurement, privacy, compliance, technology and information security should all work in a coordinated manner. Teams may require outside expertise or other resources that can operate quickly at scale. Larger organizations with frequent M&A activity should consider identifying/assigning "functional area representatives" within horizontal service and business areas, establishing repeatable processes and playbooks and trained resources in place to achieve efficiency and demonstrate a well-managed M&A process.

Accountable resources should be put in place that will be responsible for executing the agreed upon transition plan that are sufficient to resolve items within agreed upon timeframes. M&A team roles may be dedicated and centralized, or rely on participants across cross-functional areas of the organization.

While each organization has its own preferences for where specific functions are housed, and the support received from functional areas across the organization should participate in diligence and integration planning, the following guidance provides an overview of robust collaboration between the following functions will yield optimal results:

- **Finance** creates business case numbers; and critically helps to structure the type of deal, typically as an asset or stock purchase or hybrid. The level of due diligence to be performed is impacted by the type of purchase and relative level of liability that would be acquired. Financial modeling occurs for each M&A deal to define upfront purchase price and must include integration expenses.
- **Procurement** may provide a lead role in seeking insight into cost savings and synergies across all functional areas that can be gained (e.g., software/workstation licensing, reduction of duplicate staff in concert with HR, increasing business opportunity unique to the Buyer, etc.). Procurement may also provide the specialist(s) and/or analyst(s) who identify potential targets, and the contracts manager who works with the Legal department to negotiate on behalf of the acquirer and assists in ensuring due diligence is conducted.
- **Legal** should drive contract template development and negotiations, including determining what contracts are in place at the target and the implications of those agreements; the target's client base; union or other affiliations and other regulatory compliance and risk considerations, including rules for data retention/destruction during divestiture or other integration activities; and related items that are required to properly understand the full breadth of the deal and inform the final clauses/terms of the contract. Note that Legal's access to databases may allow it to identify risk based on past or current litigation, which may compromise the target's value to the acquirer.
- **Risk Management**, comprised of both TPRM and other risk management experts, should conduct assessments on behalf of the acquirer, including information security, data privacy, business continuity, disaster recovery, financial, internal controls, physical security and compliance risks.
- **Compliance** should have involvement in understanding the controls and related functions at the earliest stages of an M&A transaction – large or small – and can significantly aid the acquiring company in reducing unforeseen liabilities. The role of compliance in an M&A transaction is to assess the target company's compliance risk profile and uncover any red flags, including any past or present violations of anti-bribery laws, sanctions violations, antitrust regulations, data privacy rules, consumer protection, health and safety violations, etc.
- **Senior Management Risk Committee**, which is made up of a panel of cross-functional executives, has the objective of ongoing assessment and evaluation of applicable concerns from the deal related to the overall risk presented and its potential impact on the organization.

LEVERAGING TPRM BEST PRACTICES & TECHNIQUES

Quick-cycle assessment cycles during discovery should be agreed upon to take into account that traditional TPRM cycles are more compressed in M&A and the timeline for assessment and analysis must respond to this need. With the accelerated M&A timelines in mind, the TPRM Framework used in traditional vendor oversight processes can be successfully applied as a model to guide due diligence.

TPRM best practice areas that translate to M&A include:

- **Examining risk culture** for evidence of organizational risk sensitivity and/or lack of robust risk management hygiene.

- **Identifying red flags** rated against industry standards, regulatory guidelines and best practices.
- **Setting relevant critical risk domains** as a starting point for M&A discovery requests.
- **Assembling a comprehensive risk register** including documentation.
- **Conducting in-depth Post-Signing/ Pre-Closing assessments** to gather more complete risk information, including what Nth Parties are involved in the deal.
- **Securing commitments as a "Condition to Close"** in the deal documents (merger agreement, purchase and sale agreement, etc.).
- **Documenting new lesson learned for use in future transactions.**

Imparting Improved Structure to M&A Due Diligence

To impart much needed structure to the M&A process and allow both parties to optimize their existing resources, well-defined and proven TPRM practices can be leveraged as illustrated in Figure 2. The Guideline Tools in the appendices provide more detailed considerations by functional area and perspective (acquirer versus target).

The following are examples of techniques that can be useful in evaluating parties in M&A transactions:

Brokered Assessment Repositories and Assurance Portals
This is a type of TPRM solution that can be integrated with other risk management software and monitoring services. Brokered assessment repositories differ from individualized virtual data rooms or portals. Brokered repositories aggregate individual Nth Party assessment artifacts and results into a library, can be accessed by authorized entities. With permission from the Nth Party (in this case the M&A target), the repository provider grants requesting Outsourcers access to assessment evidence and artifacts such as pre-scoped standardized questionnaires and independent assessment reports. Users of these repositories can contribute their own assessment data and supporting documentation to the library, making the assessment process more scalable for both Outsourcers and Nth Party providers.

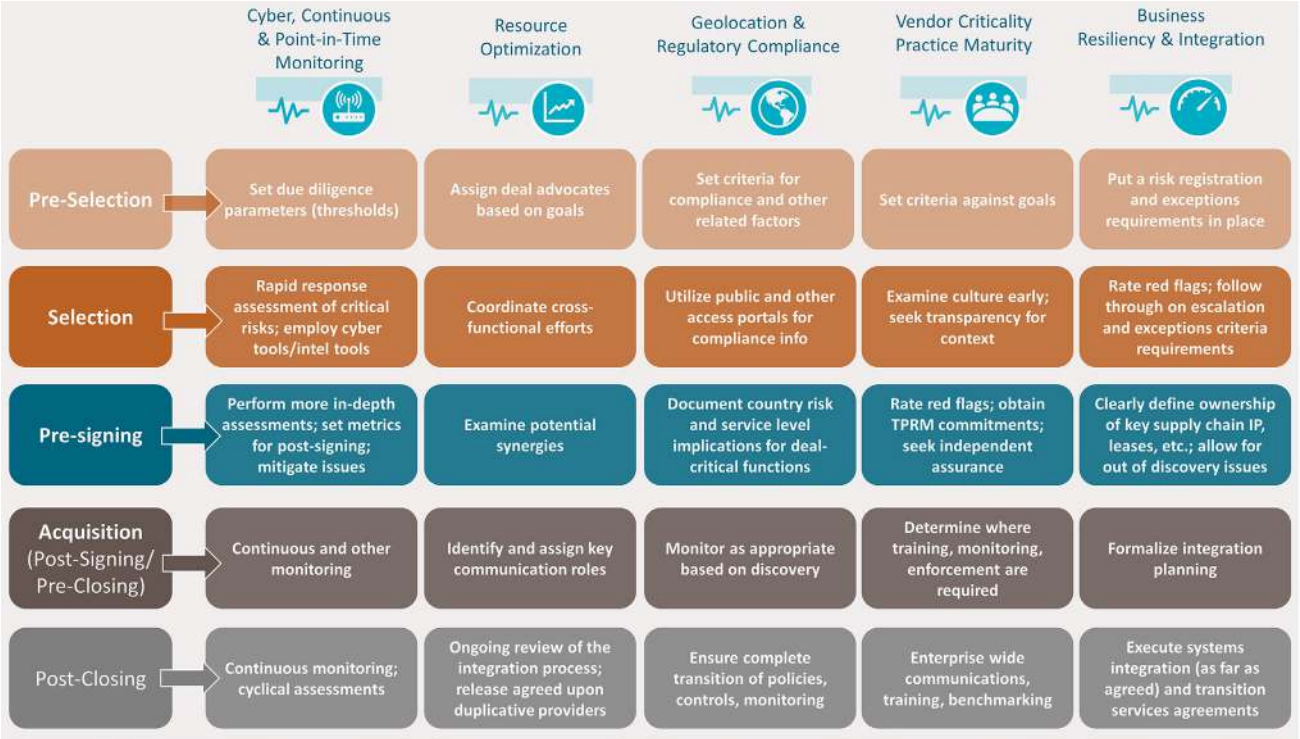
Initial Assessments and Standardized Questionnaires
Risk control domains can be used to structure topics to be assessed during due diligence. Benefits of this approach are gained when the questionnaire used reflects accurately any Reference Authority document mapping relevant to the acquirer's risk tolerance. The questionnaire can provide this risk domain alignment and evidence of the depth and breadth of the assessment. If M&A assessment process requires regulatory approval, the assessment results can be summarized to demonstrate that the deal is within the acquirer's risk appetite.

Target companies can proactively use standardized questionnaires to conduct Risk Control Self-Assessments (RCSAs) and share the results with potential M&A partners. For example, a properly scoped Shared Assessments Program Standardized Information Gathering (SIG) Questionnaire can provide baseline information for M&A by identifying topic areas where due diligence and integration planning activities need to be focused. SIG Questions are maintained by industry experts and member companies and align to specific control frameworks and regulatory expectations. They are designed to define the core risk requirements or controls for key risk topics and other high risk components (money laundering, trafficking, environment, etc.). TPRM tools cover a wide range of risk domains and typically leverage standards and regulations (e.g., ISO, FFIEC, GDPR, EBA, PCI-DSS, state and international privacy, etc.). These topics are well suited as control areas to be addressed during the M&A process.

Onsite and Virtual Assessments
As long as the two parties can agree on the evidence and method of transfer or observation, onsite validation of target controls is a vital part of managing risk. Virtual assessments can provide an alternative to onsite assessments, yielding significant productivity gains for both parties. A hybrid approach can be used by leveraging upfront virtual assessments in order to reduce the time spent onsite. Typically virtual assessments can replicate nearly any onsite procedure with the proper planning and communication.

Use of Auction Rooms
There are multiple approaches to the M&A process, including those that utilize outside investment banking, venture capital companies, or use of online auctions. M&A through auction may take place in shared data rooms with multiple bidders competing for a particular target, which compresses the timeline for assessment. Firms are competing in those settings and may be willing to employ significant manpower to win the auctions. Thoroughness is important – data provided by the target must be reliable, complete and accessible. Automated solutions provide the opportunity to assess granular detail quickly. It is important to consider all aspects of operational risk management effectiveness; financial information is not the only pivotal data to make or break a deal. The firm that wins the target in auction should retain the right to conduct further due diligence within a different platform.

LEVERAGING PRACTICES BY PHASE OF M&A



Selected best practices are shown from the acquirer's viewpoint. Target's viewpoint is reflected in this graphic by what the target will need to be prepared for and respond to during M&A due diligence discovery.

Figure 2: M&A Phases and Related TPRM Best Practices

Pre-Selection (Strategic Planning)
Pre-selection involves setting strategic criteria for a potential partner. Strategic Planning is not deal-specific. Rather, this phase frames target selection parameters for a potential M&A deal. This effort allows the rationale for any proposed deal to remain in focus. Work in this phase helps the acquirer to understand early in the process of target selection what constitutes the threshold for deal viability. Determining the type of issues that could constitute deal-breakers should be accomplished early in the planning process. Continuous monitoring solutions increasingly used in TPRM oversight can be useful to identify any deal-breaking risks that the target acquisition team has established prior to engaging with the target. And acquirers should have an escalation process in place to evaluate items that could be red flags

Assigning "deal advocates" that champion and monitor the deal has shown to be valuable in identifying any red flags and help to quantify costs and recognize synergies early in the process. Deal advocates can include use of outside advisors, as appropriate. Larger organizations may leverage financial advisors to establish the viability of the target from a business point of view. However, there are a growing number of "boutique" advisors with specific M&A expertise for many industry sectors.

This level of strategic planning requires an examination of the value that the acquirer seeks to gain from a deal. The book of business, customer value, capability and resilience all play into the decision to undertake M&A activities. For instance, the complexity of cross border activities might be determined to be too time consuming or otherwise untenable. *The importance for each party entering the market to recognize that a deficient target risk culture could be an immediate red flag cannot be overemphasized.* The risk culture of a potential target should be viewed in the context of the acquirer's own can risk appetite and culture.

Selection (Target Phase)
Within the context of the selection criteria, provisions will be laid out in this phase that will govern the acquirer's due diligence. These expectations should be formalized with a letter of intent (or other pre-signing documentation) that includes robust confidentiality terms.

The target phase includes screening, monitoring, assessing TPRM governance and culture (including compliance screening). Standardized questionnaires typically used in TPRM oversight are particularly

valuable with a willing seller as they provide a ready, pre-established, vetted and consistent means of objectively assessing a target's risk posture, including providing insight into the target's Nth Parties. By gaining an understanding of how the target handles due diligence on its own Nth Parties' providers supply chains, a wider view of the scope of risk the target presents can be gained.

In addition, provisions for post-signing assessments (including inspection of the target's supply chain) should be taken into consideration. The valuation process is part of the target selection phase. With a willing seller, the acquirer should request information directly from the target, in addition to seeking independent verification, to allow the acquirer to evaluate the target's suitability.

Even before engaging with the target, continuous monitoring techniques may identify high-level cyber or other risks that are deal-breakers or have other critical impacts. Early use of inquiry tools and techniques is recommended. For example:

- Target principals associated with nefarious activities.
- Target supply chain relies on products, services or personnel based in "prohibited countries."
- Target's external perimeter demonstrates weaknesses in its cyber security controls.

Examination of critical risks can be made through open source information sources (legal filings, complaint filings, regulatory searches, sanctions and other financial crime and appropriate watch lists). Guidelines and criteria must be adhered to that have been set up by the acquirer in the Pre-Selection phase. External audit reports and SEC filings from publicly held companies should be examined. With willing sellers, security exhibits can be obtained that provide the seller with a sense of how well a target is aligned with the acquirer's security expectation.

Due diligence efforts should go beyond commonly used testing, which can be accomplished by assessing the target's risk practices. During selection, prior compromises and their potential lingering effects should be examined. Leveraging TPRM frameworks and tools that measure a target's risk practice maturity can be helpful to drive an informed "go-no-go" business decision by the C-suite and board of directors.

Note: It is especially important that the acquirer's risk appetite statement be reexamined during the Selection phase. With a willing seller, it is possible to develop an integrated risk appetite statement during this phase.

Pre-Signing (Negotiation)
This phase includes negotiation and continued due diligence leading to a deal signing. Closing to Legal Day One in M&A equates to undertaking the same level of vetting as engaging a 'regular' incoming Nth Party provider candidate in non-M&A settings. Typically in larger mergers, LDO policy requirements that will not be in compliance on LDO across the organization must be formally documented.

A basic M&A requirement is to verify that the target's Nth Parties, clients/customers, and affiliates are inventoried (even if this inventory cannot be obtained prior to pre-signing and acquisition). These entities should be classed/rated for risk against on the acquirer's own risk management appetite.

Figure 3: Integration Planning

In early discovery, risk registers are used to document critical risks, including the extent to which compliance with relevant regulations is monitored. In-person interviews with key personnel should be conducted in each functional area to gain insight into the target partner's business, operations, risk and cyber hygiene and how risk practitioners perceive the existing risk culture. Red flags should be rated against pre-determined criteria and escalated as needed. Determinations should be made regarding the need for training, monitoring and enforcement that may be required to bring the target's culture into keeping with the acquirer's (or vice versa).

Both partners should consider putting into place enhanced data loss prevention measures during due diligence, to deter insider trading, including among staff and consultants who may have access to data sets. During due diligence, especially with smaller companies, it is sometimes difficult to achieve secure communications. For example, the use of BYOD (Bring Your Own Device) in smaller companies can lead to control issues around sensitive and otherwise confidential information. Merger participants should have a plan in place for establishing secure communication between the merger partners and advisors. In general NDAs and/or confidentiality agreements may be relied upon to cover the risk

associated with the sensitivity of the deal information). For example, it may help to define a clear initial goal, post close, such as domain whitelisting for Office 365 shared folder collaboration, with requirements such as Multi-Factor Authentication, up to date end point patching and AV/malware controls. Negotiating around requirements and required remediation early removes unplanned roadblocks to the critical first 90 days post close.

During contract negotiations, which party controls existing leases, intellectual property, union agreements/authority, and other critical items must be clearly identified and documented. A clear understanding regarding country risk and other cross border implications for deal-critical information (data sets, software licensing, leases, IP, etc.) must be achieved.

Assessment-relevant (critical) risk domains can be used as a starting point for documentation requests. Searches should be made of public information (legal filings, complaint filings, regulatory searches, sanctions and other financial crime and appropriate watch lists). Agreement should be reached on a common set of service level agreements (SLA's) to be utilized throughout the consolidated organization, including for use with Nth Party suppliers.

Note that Transition Service Agreements (TSAs) may be required when outside firms support processes that may be brought in-house or transferred to other entities. TSAs supporting contract provisions between both parties and their respective customers should be put in place. If the acquirer in the M&A is itself a Third Party provider acquiring another provider, this may result in complications that must be taken into account in TSAs. Such a relationship may add a complexity that should be explored during due diligence.

In addition, TPRM commitments should be contained in the deal documents (Merger Agreement, Purchase and Sale Agreement, etc.) that commit the seller to mitigate risks identified in due diligence as a "Condition to Close." "Representations and Warranties Insurance" intended to protect either party from inaccuracy or IT threats (such as breaches) should be considered. Contracts should require that any undisclosed discovery after closing will have a direct (quantifiable) effect on the financial terms of the deal (retroactively) to encourage transparency.

Acquisition (Post-Signing/Pre-Closing)
To better inform and correct risks prior to closing, TPRM tools and processes can be leveraged as the model for performing full onsite assessments Post-Signing and Pre-Closing. Where information is not available, compensating controls may be considered. If continuous monitoring tools used in supply chain ecosystem monitoring have not been used in diligence to date, this phase is an appropriate time to benefit from the risk indications these solutions provide. Also, remote assessment test scripts can be leveraged that are obtained through pre-closing due diligence where possible to apply a repeatable process to due diligence.

Many target sellers are amenable and will support the use of ongoing monitoring tools and techniques such as vulnerability scans, application and network PEN testing, a best practice that translates directly to the M&A space, where the acquirer would seek to perform its own PEN test prior to LDO. Findings should be documented.

Each functional area at the acquirer should draft detailed integration plans that mitigate risks identified during due diligence. Integration planning and implementation should be conducted by a carefully selected integration team comprised of both the acquirer and target subject matter experts. An integration management office should coordinate review of all integration plans for alignment and prioritize timing for execution of those plans. The goal of integration planning is to ensure 100% compliance to the acquiring organization's policies and procedures as soon after deal close as practicable.

Merger related communications should be funneled to a group of key individuals (previously identified within the combined organization) and any questions or comments should be directed to those individuals. Where outside PR firms are in place, these firms should be integrated into the communication planning and execution process to assure that messaging is consistent messaging.

Post-Closing (Integration)
The deal structure (asset purchase versus stock/cash purchase or hybrid) can impact integration activities. Integration activities Post-Close will include network, application, technology, user and password administration, testing, risk exception processes and TSA monitoring. At the Post-Closing stage, compliance activities should foot to acquirer governance policies, controls and monitoring. This is especially important in an asset purchase where there will be an additional TSA with the target performing services to the acquirer for a period of time until full conversion. In stock/cash purchase situations both the target and acquirer share risks. Contracts with both customers and suppliers can be impacted by the type of purchase since contracts may need to be renegotiated if they are not assumed by the acquiring organization, or if they do not include assignment rights.

To better anticipate impacts on the Post-Closing environment, integration plans should be constructed that are designed to achieve full compliance to the acquirer's policies and procedures by the time integration occurs. Allowances must be made for a smooth transition in the following areas:

- Nth Party supplier rationalization.
- Performance monitoring and service provision across the enterprise.

- Required ongoing monitoring, remediation (including training) to deal with unresolved issues (especially those not identified during pre-signing/closing due diligence).
- Complex system integration issues, including the use of middleware to create a single source of truth for risk management data.

Ongoing review of operations, risk management and other key areas should take place, including review of the integration process. The "out brief" guideline tool in the appendices provides a structure for reviewing the M&A action during the M&A process. An organization can tailor this tool to its own setting. This out brief provides a window into the M&A process that can be examined after the fact to determine what lessons can be learned to improve the next deal.

BENEFITS AND CONCLUSIONS

As new risks emerge and their importance is better understood, M&A due diligence must respond. This paper has examined why and how TPRM best practices can inform the overall M&A due diligence process to engender a more robust M&A process.

TPRM best practice principles can be applied broadly to relevant areas of risk that deserve examination during due diligence for any transaction, not just to those risk areas that are typically associated with Third Parties. TPRM due diligence can be uniquely adapted for application to M&A deals of all types regardless of complexity.

Key best practices are:

- **Pre-Selection:** Set strategic goals and related criteria for the deal and involve specialized deal advocates where appropriate.
- **Selection:** Coordinated efforts across enterprise provide a unified source of documentation and communications for the M&A team. Excluding targets that exceed predetermined risk thresholds.
- **Pre-Signing:** Performing intrusive, in-depth discovery, document integration plans and metrics, rating red flags and escalating as needed. Leveraging TPRM tools as a model to identify and record risks.
- **Acquisition (Post Signing/Pre-Closing):** Conducting training, monitoring, enforcement of risk management policies and procedures based on discovery as agreed during the Pre-Signing phase aligning integration and implementation plans consistent with the acquirer's risk appetite.
- **Post-Closing:** Integrating policies, controls, monitoring and reporting on LDO.

TPRM practices and tools can be used to facilitate the identification of risks and opportunities associated with a transaction. TPRM techniques in M&A due diligence may include:

- leveraging TPRM risk and control domains to inform due diligence question and target inspection;
- assessing the target company's maturity of risk governance (including TPRM functions);
- assessing the target company's risk culture;
- retesting of any existing Nth Parties that the target has engaged;
- vetting incoming Third Parties;
- examining the combined use of Nth Parties for concentration risk or other changes that might occur to the acquirer's risk profile through the acquisition; and
- examining any other redundancies or potential impacts on business continuity and resiliency.

Employing TPRM techniques to perform M&A due diligence across the enterprise is materially additive to the merger process. The TPRM lens illuminates the risk management components of an M&A deal that might otherwise be overlooked. And, TPRM tools can identify incremental risks whether companies are globally active or operate as closely held private companies.

APPENDICES – GUIDELINE TOOLS FOR PRACTITIONERS

In the M&A process, business development requests that functional area staff provide a list of scoped requests for information to the target.

Two Guidelines Tools are provided that facilitate the documentation of deal due diligence. These can be used from either partner's perspective (acquirer versus target). The tool sections can be sent to appropriate functional area representatives. These tools are designed to be used by organizations of all sizes. Typical functional areas are included in the tool. First time acquirer's would find this particularly useful as a guide. The context of an individual organization is essential to consider. These forms may be utilized in any setting, and the tool can be tailored to the needs of the organization.

Disclosure: These tools and the content of this paper are not intended to convey or constitute legal advice, is not to be acted on as such, and is not a substitute for obtaining legal advice from a qualified attorney. These tools include the strategic and tactical processes deemed the most generally applicable to and useful for the most parties, both outsourcers and targets. This material is not intended to be inclusive of every case required by statute or regulation for any specific industry, nor those mandated by any and all industry standards.

Appendix 1: Due Diligence Checklist

This tool provides insight into the functional areas that are touched during the deal, including critical services or infrastructure. Key Risk Indicators (KRIs) should be identified by the organization for activities that have the highest potential to cause significant disruption in their unique M&A setting. These KRIs would then be examined in a manner congruent with the inherent risk for that activity. The Due Diligence Checklist includes best practice considerations in the functional areas touched by each of 18 Shared Assessments' risk domains, and can be used across the five stages of M&A.

Risk Management	Incident Event and Communications Management
Security Policy	Business Resilience
Organizational Security	Compliance
Asset and Information Management	End User Device Security
Human Resources Security	Network Security
Physical and Environmental	Privacy
IT Operations Management	Threat Management
Access Control	Service Security
Application Security	Cloud Hosting

Figure 4: Shared Assessments Program 18 Risk Domains

Functional Area	Acquirer	Done or N/A	Target	Done or N/A	Notes
Risk Governance (Enterprise Risk Management)	• Document target's governing body accountably (or absence) to risk governance. • Examine target's hygiene and other compliance concerns, including business continuity for gaps. • Document target's formalized risk governance plan • Document target's formal risk metrics (or absence) and evaluation of the value of metrics. • Document formal processes target has (or absence) for processing risk exceptions and risk acceptance. • Document how target's policies and standards are aligned to industry standards (or the lack thereof). • Document how target tracks and approves exceptions and risk mitigation strategies.		• Prepare key staff and advisors overall for the sale, be ready. • Document ERM program. • Provide business continuity, disaster plans, recovery time objectives and other plans that reflect key risk indicators. • Provide assessments (overview at minimum) of Nth Party oversight policies and processes.		

Functional Area	Acquirer	Done or N/A	Target	Done or N/A	Notes
Information Security/ Privacy	• Set and document information security expectations that will be required. • Document how target privacy implications are controlled (or if controls are absent). • Document how those privacy regulations enforceable for country/region and service level risk (or if controls are absent). • Document agreed upon Transition Service Agreements (TSAs).		• Determine that policies and procedures meet industry standards and applicable regulations for the market. • Prepare and supply as needed an information security policy. • Anticipate to the degree possible interim servicing needs for buyer.		
Application Development and End User Devices	• Document any new technologies being considered for use or vetted by the acquirer that introduce unique risk. • Document target's SDLC processes (or absence of processes). • Document how targets policies and procedures for data transfer and sharing documented are enforced (or absence). • Document how SDLC includes integration and acceptance testing (or absence). • Document adequacy of targets Terms of Use, software licensing agreements maintenance, available related product and/ or service specifications.		• Determine and put in place industry standards for Software Development Life Cycle (SDLC). • Provide SDLC documentation as needed to buyer. • Document any mitigation required to meet standards during M&A.		
Network and Server Security	• Set control parameters in alignment with existing policies (or amend if more stringent policies are required for this deal). • Document agreement on those parameters (or compensating controls, if applied).		• Provide a (sanitized/redacted network diagram), showing Nth Party connections. • Document any mitigation required to meet standards during M&A.		
Human Resources Security	• Document what HR policies are in place; how those policies are communicated and regularly reviewed for compliance and other risk-related concerns (or absence thereof). • Document how integration will involve sufficient and appropriately trained and certified staff to meet control requirements. • Document target (or transitional) training provided regarding risk and employee requirements. • If required, document how tailored training will be conducted as part of integration.		• Ensure that HR policies and procedures are aligned with industry standards and applicable regulations for the market. • Provide appropriate documentation to buyer.		

Functional Area	Acquirer	Done or N/A	Target	Done or N/A	Notes
Operations Management and Resilience	• Document how people, processes, data and technology are included in risk governance plans. • Agree upon and document how integration will involve direct customer contact after close. • Determine and document all target legal rights to computing and other key assets. • Document and monitor a process owner for integration planning and review. • Document a physical security program for alignment with requirements (or absence). • Document existing formal target business continuity procedures include IT operations continuity (network operations, data center operations, call centers, etc.). • Document formal integration business continuity procedures include IT operations continuity (network operations, data center operations, call centers, etc.). • Document that key metrics (e.g., RTO/RPOs and other disaster controls such as location of backup data centers) are within acceptable limits.		• Document ERM program roles, responsibilities, processes, data controls and other key controls. • Maintain documentation on Nth Parties used. • Understand which parties will be retained or released during integration. • Communicate those roles and timelines to all parties affected. • Research key metrics required by buyer and provide related documentation.		
Legal & Compliance	• Document how the target meets required contract development, adherence and management policies and processes for its Nth Parties (or absence thereof). • Document whether country risk and service level implications controlled and enforceable. • Document target policies and procedures that identify and address bribery, corruption, and other financial crime red flags. • Document transition/integration agreed upon policies and procedures for key controls in this area.		• Inventory contracts with Nth Parties in place that provide for audit/assessment and understand and document how those can/would be transferred during integration. • Document country and service level controls. • Provide appropriate documentation to buyer.		

Appendix 2: Due Diligence Outcome Documentation

An "out brief" of the transactional due diligence phase is *typically used by the acquirer* to document risks discovered during the due diligence process and record them by functional area. This serves as a debriefing where learnings are documented. M&A and other enterprise playbooks can be updated based on the lessons learned in order to inform future M&A activities. This "out brief" can be used to guide future mergers for improved coordination of risk and related controls and streamlining M&A due diligence where inherent risk may be low. It can also demonstrate where transition planning, post-close impacts, policy exceptions, and findings from independent reviews of the deal (post close). This works in conjunction with developing and executing an integration plan. The outcome informs both the transaction (paper and deal math) and informs the integration plans (e.g., software licensing combined or type of software/applications being used post-close) and notification of risk (e.g., breach).

The tables are intended to provide guidance and are not inclusive of all concerns that may arise during M&A due diligence. The user may tailor these tools to their own setting. The tools should be used throughout the M&A lifecycle to document and facilitate the process and findings.

		Document Risks Discovered						
Functional Area	**Areas of Inspection**	**Examples of Possible Issues Identified during Due Diligence**	**Yes**	**No**	**If Yes, Synergies Identified***	**Synergy-related Costs/Gains**	**Next Steps and/ or Resolved**	**Signoff ** **
Risk Governance (Enterprise Risk Management)	Culture and Process	• The governing body was accountable to risk governance under a formalized governance plan. • Hygiene and other compliance concerns were examined for gaps, including business continuity. • Hygiene and other compliance gaps were discovered that were not remediated. • Target's policies and standards are aligned to industry standards. • Formal risk metrics (and evaluation of the value of metrics) are in place. • Risk metrics were put in place as part of integration. • A formal process for processing risk exceptions and risk acceptance is/was put in place. • Target tracks and approves exceptions and risk mitigation strategies. • If public-private merger, document any findings that indicate the target or acquirer cannot meet regulatory requirements. • Governance issues may require deal to be killed (if so, identify those issues).						

Functional Area	Areas of Inspection	Examples of Possible Issues Identified during Due Diligence	Yes	No	If Yes, Synergies Identified*	Synergy-related Costs/Gains	Next Steps and/or Resolved	Signoff **
Information Security/ Privacy	Controls and Integration	• Information security expectations have been set and documented. • Information security expectations have been communicated with the target. • Privacy implications were examined for control and enforceability for country/region and service level risk. • Connectivity was found to meet or exceed with acquirer policies and standards. • Target meets or exceeds information security KRI goals. • Target meets or exceeds privacy KRI goals met. • TSAs were designed and agreed upon with target. • Training for target and acquirer staff was conducted to facilitate TSAs and integration. • TSA were evaluated for effectiveness during implementation.						
Application Development and End User Devices	Program Transfer	• Cultural issues were identified due to lack of peer code reviews during application development. • Cultural issues were remediated as part of Closing agreement. • *Cultural issues required kill deal (if so identify).*						
	Application Development	• Target SDLC requirements have been documented. • Target policies and procedures for data transfer and sharing have been documented, are adequate and are enforced. • SDLC includes integration and acceptance testing. • Target Terms of Use are documented, software licensing agreements maintained and available related to product or service specifications.						
	Data Transfer	• Data access and transfer have been documented. • Data access (acquirer and/or target) has been provided and restricted in line with agreed upon requirements.						

Functional Area	Areas of Inspection	Examples of Possible Issues Identified during Due Diligence	Yes	No	If Yes, Synergies Identified*	Synergy-related Costs/Gains	Next Steps and/or Resolved	Signoff **
	Infrastructure Transfer	• Infrastructure was document and appropriately described. • All anticipated touch points were identified (systems solutions, data center, UI) and documented. • TSA ensured appropriate security controls remained operational. • Network connectivity and controls were reviewed and found to be aligned with requirements. • Data center facilities were inventoried, reviewed and monitored (per pre-established KRIs).						
	Application Transfer	• Analysis, planning and execution was in line with information security, privacy and other related control requirements. • Apps transfer and business functions contained necessary segregation and controls. • Post-close dependencies were identified and resolved. • All applications were successfully tested prior to LDO. • Adverse impacts were observed on customers (end users) – document if so.						
	Transition Services	• Services provided by Nth Parties were examined. • TSA framework parameters were adhered to. • If not adhered to, describe what obstacles were encountered.						
Network and Server Security		• Control parameters were brought into alignment with existing policy requirements (or amended to be more stringent if risk increased as a result of the deal).						
Human Resources Security		• HR policies were documented, communicated and regularly reviewed for compliance and other risk-related concerns. • Integration involved sufficient and appropriately trained and certified staff to meet control requirements. • Training was provided regarding risk and employee requirements (describe). • Tailored training required as part of integration was documented and provided.						

Functional Area	Areas of Inspection	Examples of Possible Issues Identified during Due Diligence	Yes	No	If Yes, Synergies Identified*	Synergy-related Costs/Gains	Next Steps and/or Resolved	Signoff **
Operations Management		• People, processes, data and technology were included in operational risk governance plans. • Legal rights were determined, inventoried and agreed upon for integration plans for all legal rights to computing and other key assets. • A process owner for integration planning and review was assigned and monitored. • The target's physical security program meet requirements. • Formal business continuity procedures were documented, including IT operations continuity (network operations, data center operations, call centers, etc.). • Where required, business continuity procedures were amended. • RTO/RPOs and other disaster controls (e.g., location of backup data centers) are within acceptable limits.						
Legal & Compliance	Reviews	• Contract reviews were conducted. • The target met required contract development, adherence and management policies and processes for its Nth Parties. • Where contract issues arose, those issues were documented and remedied. • Country risk and service level implications were examined, controlled and enforceable (if not, describe). • Policies and procedures to identify and address bribery, corruption, and other financial crime red flags are in place.						
	Policies	• Function were identified that are responsible for operational support, including policy review, production, dissemination, and (re)training. • Information security, incident response, administrative, destruction/disposal, and other relevant policy gaps were identified and documented. • Information security, incident response, administrative, destruction/disposal, and other relevant policy gaps were remedied. • Policies were updated and included in TSA?						
	Policy Exceptions	• Reviews were conducted to identify the need for exceptions (encryption removal, connectivity, authentication, etc.).						

* Synergies need to be identified ahead of consulting with the functional areas for integration planning.

** The structure and organization of sign off for responsible, accountable, consulted (RAC) or other appropriate construct would be enterprise-dependent; however, it should be clearly documented.

Acknowledgments

This is one in a series of Shared Assessments Program resources on best practices in Third Party Risk Management. We'd like to thank the Shared Assessments volunteer subcommittee members and other TPRM thought leaders who conducted and contributed to this effort. This is a group of volunteers from a wide range of Shared Assessments groups, including Best Practices TPRM & Assurance Awareness Group, Regulatory Compliance & Audit Awareness Group, Privacy Committee, Tool Development Committees, Financial Vertical Strategy Group and the Insurance Vertical Strategy Group.

- **Philip Bennett**, Manager Information Security, Metrics & Analytics, Navy Federal Credit Union; Group Chair for M&A Project; member Shared Assessments Financial Institutions Vertical Strategy Group
- **Renee Forney**, Senior Director of Cyber Assurance, Capital One, member Shared Assessments Advisory Board
- **Sridhar Gundrothu**, Senior Manager, Cyber Security and IT Risk, Genpact USA; member Shared Assessments Best Practices Committee, CM Working Group, OTRM Group, Privacy Committee, Regulatory Compliance Committee, SCA/SIG/VRMMM Committees
- **David Hubley**, Cyber | Director - Information Assurance Third Party Management, Capital One; member Shared Assessments Steering Committee, former SCA Committee member
- **Kaelyn Lewis**, Senior Risk Analyst, Rochdale Paragon (apogee IQ); member Shared Assessments Best Practices Committee, CM Working Group, Regulatory Compliance Committee
- **Tony Mastrolembo**, Vendor Risk Management (VRM) Program Manager, Freddie Mac; Co-Chair Regulatory Compliance Awareness Group, member Best Practices Committee, former VRMMM Committee member
- **Linnea Solem**, President & Founder, Solem Risk Partners LLC ; member Shared Assessments Advisory Board and liaison to the Shared Assessments Steering Committee
- **Christopher Wancko**, IT Strategy Senior Advisor, Cigna; member Shared Assessments FI Vertical Strategy Group

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this effort:

- **Jeremy Byellin**, Vice President, Legal and Regulatory Affairs
- **Bob Jones**, Senior Advisor; Staff Lead, Shared Assessments Best Practices Awareness Group
- **Brad Keller**, Senior Vice President & CSO
- **Mike Jordan**, Vice President, Research
- **Charlie Miller**, Senior Advisor; Staff Lead, Shared Assessments Continuous Monitoring Working Group, Operational Technology Risk Management Group, and Insurance Vertical Strategy Group
- **Gary Roboff**, Senior Advisor; Staff Lead, Shared Assessments Regulatory Compliance Awareness Group
- **Marya Roddis**, Vice President, Technical Writing, Editor
- **Rella Rivera**, Executive Assistant

ABOUT THE SHARED ASSESSMENTS PROGRAM

As the only organization that has uniquely positioned and developed standardized resources to bring efficiencies to the market for more than a decade, the Shared Assessments Program has become the trusted source in Third Party risk assurance. Shared Assessments offers opportunities for members to address global risk management challenges through committees, awareness groups, interest groups and special projects. 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. The Shared Assessments Program is managed by The Santa Fe Group, a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit: http://www.sharedassessments.org.

ENDNOTES

i 2019 Global M&A Outlook: Unlocking value in a dynamic market. January 2019. J.P Morgan. https://www.jpmorgan.com/jpmpdf/1320746694177.pdf; Q4 and full-year 2019 update: Rebound or retreat? Dealmakers navigate a hazy economic forecast as 2020. PwC. https://www.pwc.com/us/en/services/deals/industry-insights.html

ii Statement on privacy implications of mergers, Adopted 19 February 2020. European Data Protection Board (EDPB). https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf; Statement of the EDPB on the data protection impacts of economic concentration. Adopted 28 August 2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_economic_concentration_en.pdf