SFG

SHARED ASSESSMENTS

The Trusted Source in Third Party Risk Management

THIRD PARTY CONTRACT DEVELOPMENT, ADHERENCE & MANAGEMENT

TABLE OF CONTENTS

SFG | SHARED ASSESSMENTS

BUILDING BEST PRACTICES:

Third Party Contract Development, Adherence & Management

Introduction

This paper documents best practices for streamlining third party contract development, approval, exceptions and addendums processes. Organizations increasingly rely on contract clauses and policies to mitigate third party risk. However, fewer than half in a recent study reported they are able to monitor compliance with contract provisions.[i] This paper examines the need for actionable contracts and shows how they can be written and managed across the relationship lifecycle from both the outsourcer and third party provider perspectives.[ii]

Three areas of contract management across the third party relationship lifecycle are examined:

- New Relationships.
- Existing Relationships, including Evergreen Contracts.[iii]
- Renewals and Terminations.

The contract development and management process is shown to be most effective when the outsourcer and its third party work as a team. When a well-developed best practice is unified across the enterprise, it provides a documented, defensible approach to contract management throughout the third party lifecycle. Other benefits of a consistently applied contracting process include:

- Overall strengthening of risk governance throughout the enterprise.
- Improved relationships through the use of individualized risk ratings and actual assessment results to drive processes.
- Possible reduction in current and future legal and regulatory compliance costs for both parties.

Unique considerations exist around specific industry relationships, such as health care, financial services or assessing security and controls for public cloud provider use. Examples are provided in the *Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage.*

Disclaimer: The information presented in this document are offered for informational purposes only. It is 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.

Threat Landscape

Contract development and management due diligence techniques are demanding closer scrutiny of a number of factors that affect the establishment and ongoing maintenance and monitoring of relationships with third parties (and, where possible, to nth parties). Pertinent examples of directives and emerging best practices around third party contract management are contained in *Appendix 9: Examples of Regulations and Industry Standards Surrounding Contract Management.* Most notably, many regulatory agencies have mandated senior management obtain board approval before execution of any contract in which the third party relationship is deemed to involve "critical" activities. Other changes to the threat landscape and regulatory mandates that highlighting areas of contract management which require extra diligence include addressing:

- Right to audit, assess and monitor;
- Material changes to services and/or products being provided;
- Risks surrounding emerging technologies (IoT, AI, Robotics, etc.);
- Geolocation and other infrastructure risks;
- Establishment and renewal of evergreen contracts; and
- Merger and acquisition (M&A) activities.

Contract controls are being relied upon at many levels throughout the third party risk management lifecycle to meet the requirements of existing and emerging regulations and standards. This is demonstrated in the *2017 Shared Assessments' Vendor Risk Management Benchmark Survey*, where the Contracts category showed improvement since 2015, yet a decline was seen in having a defined (and therefore effective) organizational structure for third party contract drafting, negotiation and approval. In the Shared Assessments' *Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk*, twice as many outsourcing organizations (75%) reported they rely on controls of their third party to monitor fourth parties than two years ago; and 73% reported they use contractual terms to achieve this process. *Yet - while most organizations reported relying on contract clauses and policies to mitigate third party IoT risk; fewer than half are able to monitor their third parties' contract compliance.*[vi]

Together, these results demonstrate the need to address certain third party issues upfront in the contract, enabling outsourcers to proactively address risks posed by third party relationships. These findings also show the need for clear communications during contract development to ensure that third parties have realistic (achievable) expectations for meeting contract requirements.

Documenting Emerging Best Practices in Contract Management

Contracts is an area of third party risk management where the incorporation of standardized terms has the potential to enable more effective third party risk management. *Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage* contains specific suggestions for contract provisions and clauses that can be used to help tailor an organization's contract templates. These standardized terms should be based on a well-documented risk appetite framework that operates coherently at all levels across the enterprise. A third party risk management program that has a team-based standardized contract development process that works in concert with Procurement is considered the best practice approach for successful implementation.[vii] Such an approach ensures that both Procurement and the business units are aware of risks identified as part of the assessment process. Utilizing this methodology increases the ability for outsourcers to examine third party controls prior to execution of the contract. This approach also provides assurance that the third party is aligned with the standards of the outsourcer and gives the third party an indication of what to expect and the periodicity (frequency) of the assessments the outsourcer will conduct.[viii]

The role of due diligence is to ascertain whether or not the inherent and residual risk presented by the third party is consistent with the outsourcer's risk appetite. Due diligence standards for contracting should reflect:

- The type of services being outsourced.
- The type(s) of data and critical assets being touched by the third party provider.
- The regulatory environment surrounding service, data and access.
- The use of actual due diligence findings to guide a determination of how the organization's security standards need to be reflected in contracts, Master Services Agreements (MSAs), Statements of Work (SOWs) and Service Level Agreements (SLAs).

The outsourcer should fully understand: 1) the inherent risks presented by allowing the third party to have access to its sensitive customer and proprietary information; and 2) the potential impact that performance of the services on the outsourcer's behalf may have on the outsourcer. Therefore, it is important for the outsourcer to think broadly about the type and severity of risks an outsourcing decision might introduce, including resiliency and recovery-related concerns.

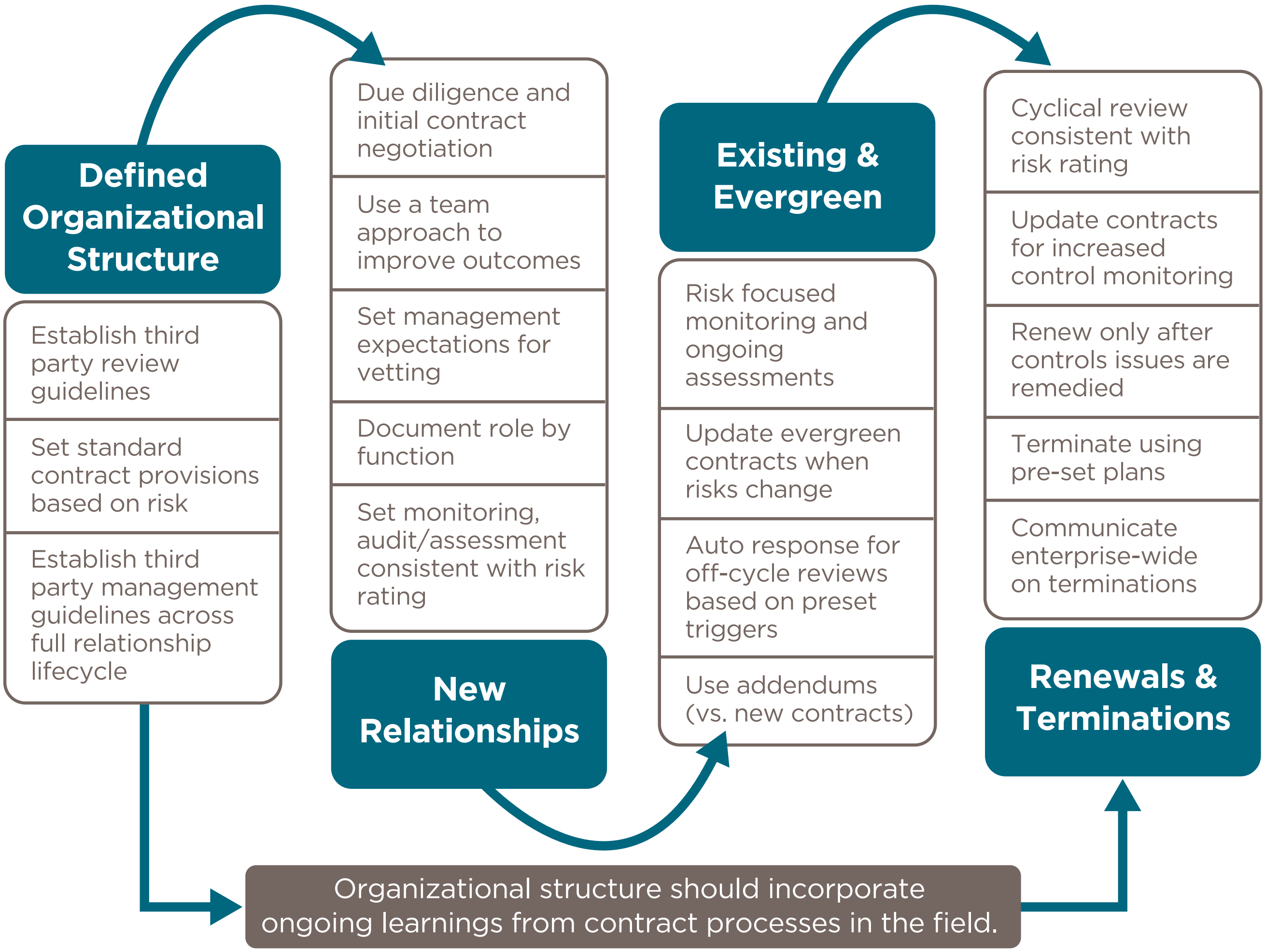
Once a third party has been identified and the contracting process has begun, SOWs should be clearly defined, and a risk profile should be created for the prospective provider that is tied to this SOW. This profile should include a series of questions the outsourcer needs to answer about the service provider in order to determine an initial (tentative) risk rating for the third party. This rating will be the foundation for the type of due diligence performed on the prospective provider. The results of that due diligence yield a clearer view of the outsourced activity risk rating (the inherent risk of the activity) that the outsourcer can then choose to mitigate, transfer, avoid (i.e., not accept) or accept. In turn, the SOW will drive the SLAs required for governing the relationship.

No matter which level of due diligence is performed on the service provider, it should incorporate elements across each of the 18 risk domains listed in *Appendix 2: Shared Assessments Standardized Information Gathering (SIG) Questionnaire & Standardized Control Assessment (SCA) Procedures Risk Domains*. Requirements related to each of these domains should be clearly defined in the contract, so that the service provider is aware of the expectations of the outsourcer and knowledgeable of the specific standards with which the third party will be required to comply. Both parties should have their relevant teams review the requirements and ensure the correct language has been incorporated into the contract and that the standards are achievable. In other words, the third party should have the infrastructure, controls and processes in place that will allow them to meet the terms of the contract.

Developing and Managing the Contract Across the Lifecycle

Best practices dictate that risk-based evaluation of providers is based on the actual risk posed (i.e., the residual risk after controls are applied; and the inherent risk, should those controls fail). The policies, procedures and processes for this risk rating (tiering) should be documented in the overall third party risk management program. Most importantly, risk rating and related contract development processes should be repeatable, scalable and monitored across the life of the contract.

Contract best practices across the third party lifecycle that are proving successful in moving the needle on risk management include:



Defined Organizational Structure

- Establish third party review guidelines
- Set standard contract provisions based on risk
- Establish third party management guidelines across full relationship lifecycle

New Relationships

- Due diligence and initial contract negotiation
- Use a team approach to improve outcomes
- Set management expectations for vetting
- Document role by function
- Set monitoring, audit/assessment consistent with risk rating

Existing & Evergreen

- Risk focused monitoring and ongoing assessments
- Update evergreen contracts when risks change
- Auto response for off-cycle reviews based on preset triggers
- Use addendums (vs. new contracts)

Renewals & Terminations

- Cyclical review consistent with risk rating
- Update contracts for increased control monitoring
- Renew only after controls issues are remedied
- Terminate using pre-set plans
- Communicate enterprise-wide on terminations

Organizational structure should incorporate ongoing learnings from contract processes in the field.

Figure 1: Contract Best Practices Across the Third Party Relationship Lifecycle

Establishing Review Guidelines for Third Parties

The outsourcer and the third party should agree upon the items listed below and develop a strategy and mechanism to document these guidelines:

- Metrics, monitoring and reporting requirements.
- Point at which the outsourcer will reevaluate the contract.
- MSAs, SOWs, SLAs and/or other governing points for contract development.

Examples of guidelines for establishing review criteria within the contract environment may include:

- Establishing and monitoring performance standards.
- Establishing criteria for the contract review cycle consistent with each tier of the third party risk classification/rating.
- Definition of confidential information and how it is designated.
- Business continuity planning requirements that include disaster recovery and business continuity for infrastructure and people-driven processes.
- Incident management and communications criteria.

The Shared Assessments *Vendor Risk Management Maturity Model (VRMMM)* provides third party risk managers with a tool that can be used to evaluate their program against a comprehensive set of best practices. The VRMMM highlights two critical steps for achieving maturity in contracts management:

- Establish third party contract management processes that are mission-driven.
- Establish criteria for the alignment of contracts with the outsourcer's third party risk classification structure.

Setting Contract Guidelines

Contract guidelines are an essential element in all third party risk management programs, regardless of the type or size of the outsourcing organization. All organizations need to establish such guidelines to ensure their third party contracts cover key risk areas unique to their situation, their industry and the activity being outsourced. Guidelines that follow well-vetted processes and establish enforceable risk performance requirements, including right to monitor and otherwise audit, are essential to robust risk management. *Any exceptions to guidelines should be deliberated with due care and should be approved by the appropriate executive management prior to execution of a contract.*

The degree of assurance required in any assessment will be a function of an activity's inherent risk, the risk tolerance associated with a specific activity and the third party's risk profile. In some industries (e.g., financial services) contracts for outsourcing of so-called "critical" activities may require regulatory mandated levels of assurance. Contracts should be written in a manner that clearly defines the provider's requirement to comply with the outsourcer's operational and security standards. Contracts should also provide details related to SLAs and the expectations regarding the act of outsourcing to a fourth party (i.e., the third party's subcontractor and the service provider's third party risk management program[ix]). A positive trend in this direction was shown in the *2017 Shared Assessments' Vendor Risk Management Benchmark Survey*, in which respondents indicated progress in defining these terms within their contracts. And yet, more than half of respondents said they planned to de-risk in the next two years, and an inability to monitor fourth party security hygiene was the top reason why.[x]

Pre-onboarding policies that address considerations and procedures internally should be documented so that they are applied before entering into a contract. This can include a standardized pre-onboarding questionnaire for all business units that wish to outsource, so that risk is evaluated on a consistent basis. Standard contract language in the main contract and allowing for addendums over time simplifies the contracting process and allows for easier negotiations for the outsourcer for renewals and evergreen contracts.

One of the major areas of opportunity for change within contract management is the inclusion of language regarding the outsourcer's right to audit the third party provider. Due to regulatory scrutiny this concern has been brought to the forefront of third party risk management. The inclusion of a right to audit clause has emerged as the number one best practice in contract management. A right to audit clause enables an outsourcer to take a proactive approach to quantifying and monitoring the effectiveness of controls to protect against the inherent risks associated with a specific engagement service provider. The clause should not only address the best practice of assessing all third parties and the frequency, it should also identify specifically what the outsourcer may audit.

Provisions controlling an outsourcer's audit rights should include:

- A right to audit clause to:
  - Ensure the ability of the outsourcer to perform robust audits on the third party for investigations of any claims of breach of contract, misappropriation, fraud or business irregularity of a potentially criminal nature; audits required by governmental or regulatory authorities; due diligence and periodic assessments.
  - Define the artifacts that need to be provided as support of the assessment of controls and on site reviews.
  - Address the inclusion of parameters for ongoing and continuous monitoring of the risk posed by the provider.

- A “right to investigate” clause should:
    - Authorize the outsourcer to conduct an examination in the case of any anomaly, including declaration of a breach of contract at the third party, or its subcontractor, to determine if an investigation is warranted.
    - Include terms that express a preference for the use of a mutually agreed upon forensic investigator.
    - Include terms that guarantee outsourcer access to reports if the outsourcer agrees to allow the third party to retain a forensic investigator to conduct the investigation.
    - Include terms that guarantee the service provider access to the results of any forensic investigation initiated by the outsourcer.

Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage contains specific suggestions for contract provisions and clauses that can be used to help tailor an organization’s contract templates. Some key examples of contract guidelines beyond right to audit and assess include:

- Boilerplate contract terms and/or SLAs that can be modified by the provider to include requirements of a risk management program at the third party level that is consistent with the outsourcer’s risk tolerance.
- Provisions controlling:
    - Clear and complete definition of the services provided and role of the parties.
    - 24x7 SLAs with specific failure to comply clauses.
    - Service Oriented Architectures (SOAs) clarifying where services will be provided by application components over a network and the communication protocols that will be used to do so.
    - Geolocation and security of data (offshore/onshore or encrypted in transit or at rest), as applicable.
    - Business Continuity Planning (BCP) requirements tied to the needs of the outsourcer and the risk posed by the provider.
    - Information Security, Privacy and Confidentiality requirements, with defined data access limits.
    - Documented security and data breach notification and resolution processes with provider notifications to outsourcer by issue type and within specified timeframes.
    - Compliance with applicable laws and regulations.
    - Cybersecurity assurances, such as cyber insurance, where appropriate.
    - A subcontractor clause that covers the use of downstream contractors by the outsourcer’s third parties.
    - Agreement assignment (provisions for the sale or discontinuance of a business(es) by either party, etc.).
    - Clearly defined escalation processes tied to pre-determined (documented at a point-in-time) industry standards.
    - A well-defined exit strategy.

Control questions, such as those in the Shared Assessments SIG questionnaire and the VRMMM, can be restated as control capabilities and inserted into a contract as an appendix.

It is of particular note that issues may arise whenever the contract authors do not understand that if a specific term is not taken into account in contract language and prohibited or controlled, the other party may by default have permission to do something not included in the contract language. Given that this circumstance could cover a wide variety of issues, the review of the contract should include a recheck of items initially included in the contract but removed or edited during the negotiation process do not violate key provision requirements for either party.

Contract Development & Management Lifecycle Stages

Three areas across the third party relationship lifecycle are examined in this paper:

- New Relationships.
- Monitoring of Existing Relationships.
- Cyclical Reviews for Terminations, Renewals and Evergreen Contracts.

New Relationships

Appendix 4: Sample Third Party Selection Criteria provides specific examples of review criteria and related techniques.

<u>Due Diligence & Initial Contract Negotiation</u>

To strengthen contract language and enforceability, best practice dictates a strong standard for risk management agreed upon by all stakeholders *<u>before</u>* a third party is brought on board. By consistently involving all relevant team participants (e.g., Procurement, Business Units, Risk Management, Security, Business Resiliency, Privacy and Legal) in the third party onboarding process, the teams can collectively establish a standard internal process for handling all types of third parties.

<u>Setting Management Expectations</u>

Setting parameters at the outset of contracting with a third party provides a solid foundation for the success of any program. Key contract dates, business owners and specific vetting indicators for what will be assessed should be included at this stage. Due diligence may include, but should not be limited to: financial viability, reputation, references, licensing requirements, insurance coverage, past/existing judgment or sanctions disclosure and regulatory requirements specific to the relationship.[xi]

Role by Function

The contract development and management process is most effective when the outsourcer and its third party work as a team. In the majority of organizations with very mature contract management processes, contracts are drafted, monitored and maintained with participation from the following departments:

- Legal and Compliance: Draft and/or review the contracts to ensure all necessary points are included.
- Business Units: Assist in contract negotiations, development of performance metrics and SLAs, RTOs (Recovery Time Objectives), RPOs (Recovery Point Objectives) and Recovery Capacity, business continuity plans, initiate due diligence processes, and collaborate with other enterprise areas for review and follow up activities.
- Procurement: Leads contract negotiations, assists in development of performance metrics and SLAs, and coordinates with legal and business units to finalize contracts.
- Third Party Risk Management and Oversight: Where applicable, drive validation of third party controls, processes and procedures and drives the risk assessment processes for relationships where initial due diligence indicates further review is required and ensures Procurement and the business units are aware of risks identified as part of the assessment process.[xii]
- **Note:** In some industries, when critical activities are outsourced, a senior management team member may be required to oversee the contracting process.

Existing Relationships & Evergreen Contracts

Existing relationships should be examined on a regular basis, with reviews taking place when trigger events occur at off-review-cycle times. *Appendix 5: Sample Monitoring Criteria for Existing and Evergreen Contracts* contains additional examples of key criteria and related techniques for monitoring.

Contract Monitoring & Ongoing Assessments

For existing contracts, criteria should be established that determine contract review cycles are consistent with the current risk rating of the provider (risk ratings should be updated at regular intervals). For evergreen contracts, the relationship owner should periodically refresh the risk rating of the relationship (timing should be based on an assessment of the inherent and residual risks of the engagement) and respond accordingly to any change in risk level.

Procedures should be put into place for review of existing contracts for compliance with current contract standards, and with remediation processes to correct contract deficiencies. *Right to audit performance requirements that are contractually enforceable are key to both setting expectations and obtaining ongoing information that third party relationships managers rely upon for effective relationship monitoring.* Considerations for monitoring and response should be already built into new contracts. For existing relationships, where these expectations have not yet been set, risk assessments would be performed at previously agreed upon levels, with the outsourcer recognizing opportunities that may exist for contract revisions or amendments at predefined trigger points, such as a change in the provider's scope of work.

Key contract obligations should be reviewed at account management meetings, such as where data is stored and processed, whether or not fourth parties are

Level of Assurance Guidance based on Risk Rating

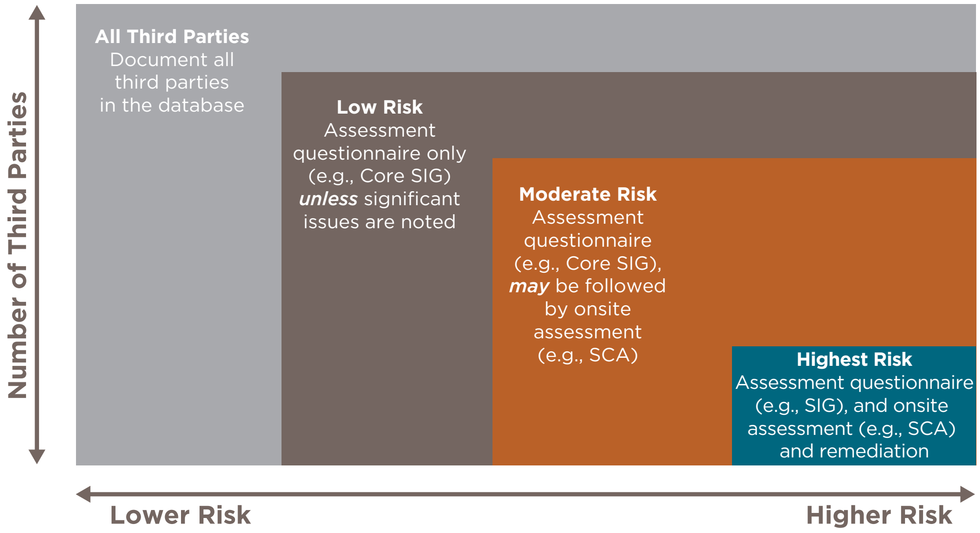

Number of Third Parties
All Third Parties
Document all third parties in the database
Low Risk
Assessment questionnaire only (e.g., Core SIG) *unless* significant issues are noted
Moderate Risk
Assessment questionnaire (e.g., Core SIG), *may* be followed by onsite assessment (e.g., SCA)
Highest Risk
Assessment questionnaire (e.g., SIG), and onsite assessment (e.g., SCA) and remediation
Lower Risk
Higher Risk

Figure 2: Monitoring & Assessment Levels Based on Risk

involved, production and data center location changes, and any changes to mission critical functions and/or staffing. Best practices dictate that meetings be held at regular, pre-established intervals, with the timing of reviews tied to the provider's risk rating and reviewed at specific trigger and escalation points. Monitoring at the fourth party level can be set up to require documented evidence, such as industry certifications and independent assessments, of how third parties monitor their fourth party risk posture assurances.[xiii]

Monitoring should always be appropriate to the relationship (i.e., based on the risk focused) and, at best, cost effective for both parties. Contract language should enable ongoing or continuous monitoring of both third and fourth parties in sensitive areas, with obligations to disclose any adverse event occurrences, litigation or customer complaints to the outsourcer.[xiv] For existing contracts which lack a right to audit clause, an addendum may be negotiated for that language, as well as for any regulatory changes if those are not automatically included under the contract through existing language.

Setting Triggers for Contract Changes

Use of a contract template will help establish an enforceable standard that can be evaluated for effectiveness by providing consistent feedback that can be updated across the enterprise more efficiently. Templates should be configured to include critical elements of an established set of outsourcing criteria and inclusion of pertinent SLAs, Key Control Indicators (KCIs), Key Performance Indicators (KPIs), Objective and Key Results (OKR) Indicators, level of assessment, assessment cadence and other relevant requirements. Clauses can be boiler plate, using a playbook approach to guide use according to risk rating, provider and/or service/product type.

Defined triggers should require an automatic notification to a predefined position at the outsourcer that would typically initiate a specific due diligence process. For higher risk third parties, periodic reviews and updates, as needed, to Master Services Agreements (MSA) ensure both parties are aware of changes in third party processes or other organizational considerations that may mandate changes to the contract and/or addendum. Therefore, outsourcers should meet with their third parties often.

Unique concerns exist around specific industry relationships, such as healthcare, financial services or assessing security and controls for public cloud provider use. Examples of specific triggers are provided in *Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage*. Best practices around due diligence and contract management for cloud provider relationships are discussed in more detail in *Evaluating Cloud Risk for the Enterprise – An Updated Shared Assessments Guide and Assessment of Public Cloud Computing Vendors*. Regardless of what triggers are used, an alert or other tracking mechanism should be created and maintained within the vendor inventory for expiry dates of contracts and other review cycle triggers.

Use of Addendums versus Novation (New Contracts)

An outsourcer should determine the point(s) where it can make use of addendums versus needing to renegotiate a new contract. This decision should be based upon pre-agreed metrics and/or reporting requirements that are documented and communicated across the outsourcer's enterprise. In some cases, changes in regulations or sanctions can require contracts to be terminated if amendment through addendum is otherwise not possible. An example of this is the European Union (EU) General Data Protection Regulation (GDPR) requirements governing contracting between Data Controllers (outsourcers) and Data Processors (providers). If a relationship is already in existence when such a regulation takes effect, that would need to be accounted for in an addendum, or otherwise dealt with to ensure that the third party meets the same requirements that apply to the outsourcer. In part, GDPR Article 28 Privacy provisions require a contract when a controller uses a processor, and when a processor uses a sub-processor. Terms and conditions of controller to processor contracts should flow down to sub-processors. For international transfers of Personal Data from the EU, specify the legitimizing method utilized: e.g., model contracts/clauses, binding corporate rules, Privacy Shield, adequate country designation. Contracts should set out the subject matter of the processing; duration of the processing; geolocation and nature and purpose of the processing; and type of personal data and categories of data subject.[xv] For other examples of requirements, see *Appendix 9: Examples of Regulations and Industry Standards Surrounding Contract Management*.

Contract Renewals & Terminations

Cyclical Reviews for Contracts

Pre-established plans should be in place to ensure that when a third party should be terminated and/or replaced, contingency plans allow for business continuity and resiliency in the event that products and/or services become unavailable from the original third party. This planning is based on examination of the dependency and any concentration risk presented by the outsourcer's third party providers.[xvi]

Updating Contracts

Before renewing or expanding any contract, existing providers should be required to address any material issues that have arisen during monitoring (yet have not required prior termination or remediation based on existing contract requirements). Other considerations included in *Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage* in the Appendices are: changes in scope of services; changes in risk profile require changes to oversight activates; periodic refresh of due diligence;

onsite review; and right to audit specific to a risk domain (business continuity, disaster technology recovery, security). Mergers and acquisitions (M&A) is a unique area of contract consideration, including due diligence during the M&A process. Some examples of considerations for M&A situations are listed in *Appendix 7: Sample Mergers and acquisitions (M&A) Contract Considerations*.

Terminations & Communications on Terminations

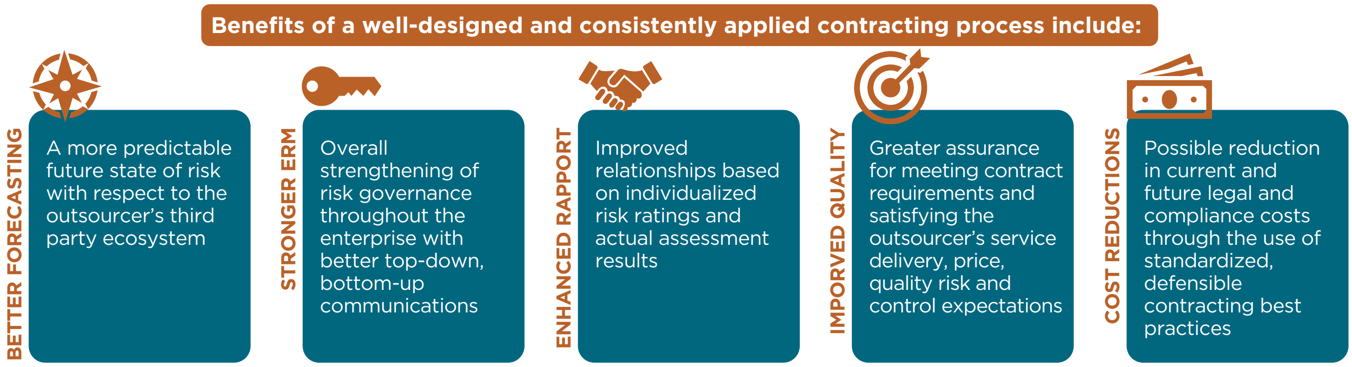
A few examples of third party provider relationship management challenges to achieving good risk management hygiene during the Renewal and Termination stages include:

- Document the termination in the third party database and communicate the reason(s) for termination. Procurement and other business units will have this information available for other existing contracts with the provider and for future reference.
- If termination was for cause, document the root causes:
    - Was the provider appropriately rated?
    - Did controls fail?
    - Are there monitoring, control logs, evidence?
- Termination that occurs by contract provision (reaches the end of the contract term). Wind down, document using a pre-defined exit strategy.
- Ensure there is no service disruption during the winding down period.
- Recover any and all fourth party subcontractor or licensee data or confirm in writing that secure data destruction has taken place.
- Ensure that proper notice of termination or non-renewal is sent.

Additional examples are available in *Appendix 6: Sample Renewal Update or Termination Criteria*.

Summary of Benefits & Conclusion

Robust contract development practices provide benefits for both the outsourcer and the third party provider. The contract development and management process is most effective when the outsourcer and third party work as a team. A formal contracting process demonstrates best practice when it includes template/boiler plate language specific to third party relationships. It is productive for both parties to understand the negotiation of contracts from the other party's perspective and work to remediate risk issues in a cost-effective manner while ensuring that contract requirements remain aligned with the outsourcer's risk appetite. When a well-developed, unified approach is applied across the enterprise, it provides a documented, defensible approach to contract management throughout the third party lifecycle.



Benefits of a well-designed and consistently applied contracting process include:

BETTER FORECASTING
A more predictable future state of risk with respect to the outsourcer's third party ecosystem

STRONGER ERM
Overall strengthening of risk governance throughout the enterprise with better top-down, bottom-up communications

ENHANCED RAPPORT
Improved relationships based on individualized risk ratings and actual assessment results

IMPORVED QUALITY
Greater assurance for meeting contract requirements and satisfying the outsourcer's service delivery, price, quality risk and control expectations

COST REDUCTIONS
Possible reduction in current and future legal and compliance costs through the use of standardized, defensible contracting best practices

Figure 3: Benefits of Applying Contract Processes Best Practices

ENDNOTES

i *Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk.* Ponemon Institute and The Santa Fe Group, Shared Assessments Program. 2018.

ii Parties within this paper are defined as: Outsourcer – the entity delegating a function to a subcontractor; Third Party – the subcontractor for the outsourcer; Fourth Party – a subcontractor to the outsourcer's third party, regardless of whether the fourth party has a potential materiality/criticality impact on the original outsourcer.

iii An Evergreen contract is one in which both parties have agreed to automatically renew the contract after each maturity period, unless formally terminated under the existing provisions of the contract.

iv *Vendor Risk Management Benchmark Annual Survey.* Protiviti, Inc. and The Santa Fe Group, Shared Assessments Program. December 2017. The Maturity Level on a 0-5 point scale for Contracts was 3.1 in 2017, up from 2.9 in 2015. 3.0 is defined as: the organization has fully defined, approved and established vendor risk management activity, but it is not yet fully operational. Metrics and enforcement are not yet fully in place.

v *Shifting toward maturity: Key findings from EY's 2016 financial services third-party risk management survey.* EY. June 2016.

vi *Second Annual Study on the Internet of Things (IoT): A New Era of Third-Party Risk.* Ponemon Institute and The Santa Fe Group, Shared Assessments Program. 2018.

vii *Building Best Practices in Third Party Risk Management: Involving Procurement.* Shared Assessments Program. 2016.

viii Third Party Risk Management (TPRM) Framework Shared Assessments 2018 Pre-Summit Workshop. The Santa Fe Group, Shared Assessments Program. April 2018. John Bree, SVP & Partner (Neo Group) & Christopher Murphey, Client Partner (Rsam).

ix Parties within this paper are defined as: Outsourcer – the entity delegating a function to a subcontractor; Third Party – the subcontractor for the outsourcer; Fourth Party – a subcontractor to the outsourcer's third party, regardless of whether the fourth party has a potential materiality/criticality impact on the original outsourcer.

x *Vendor Risk Management Benchmark Annual Survey.* Protiviti, Inc. and The Santa Fe Group, Shared Assessments Program. 2017.

xi *Risk Rating Third Parties: Optimizing Risk Management Outcomes.* The Santa Fe Group, Shared Assessments Program. 2017.

xii Third Party Risk Management (TPRM) Framework Shared Assessments 2018 Pre-Summit Workshop. The Santa Fe Group, Shared Assessments Program. April 2018. John Bree, SVP & Partner (Neo Group) & Christopher Murphey, Client Partner (Rsam).

xiii *Fourth Party Risk Management: Supply Chain Issues and Emerging Best Practices.* The Santa Fe Group, Shared Assessments Program. 2017.

xiv *Continuous Monitoring of Third Party Vendors: Building Best Practices.* The Santa Fe Group, Shared Assessments Program. 2017.

xv *Appendix: Article 28 Contract Considerations General Data Protection Regulation (GDPR): Data Processor Privacy Tool Kit.* 2018 Program Tool and Template Set.

xvi In the outsourcing context, concentration risk can be defined as the probability of loss arising from a lack of diversification. BITS Guide to Concentration Risk in Outsourcing Relationships. BITS. 2010.

xvii *Vendor Risk Management Benchmark Annual Survey.* Protiviti, Inc. and The Santa Fe Group, Shared Assessments Program. 2017.

xviii Such as, Shared Assessments' Standardized Control Assessment (SCA) SCA Privacy Testing Procedures (formerly the Shared Assessments' AUP) and/or Service Organization Control (SOC) 2 or International Standard on Assurance Engagements (ISAE) 3402.

xix Demystifying China Cybersecurity Law. Protiviti, Inc. March 2018.

xx *FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs.* April 2018; *FFIEC Information Technology Examination Handbook. Appendix J: Strengthening the Resilience of Outsourced Technology Services.* FFIEC. February 2015.

xxi *Third-Party Relationship: Supplemental Examination Procedures Bulletin.* OCC 2017-7. January 2017.

xxii Bulletin 2013-29. Third-Party Relationships: Risk Management Guidance. OCC. October 2013; Bulletin 2001-47 Third-Party Relationship Risk Management Principles. November 2001.

xxiii *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information.* Company Association of Corporate Counsel (ACC). 2017.

xxiv *Cybersecurity Legal Task Force Vendor Contracting Project: Cybersecurity Checklist.* American Bar Association (ABA). November 2016.

xxv *Principles for Fair and Accurate Security Ratings.* US Chamber of Commerce. June 2017.

Acknowledgments - Thank You to Our Best Practices Awareness Group

This is one of many briefing papers within a series of best practices in third party risk management. We'd like to thank the Shared Assessments Best Practices Group volunteer subcommittee members who conducted this effort:

- **Mike Blair**, Manager of Vendor Oversight, Early Warning
- **Angela Dogan**, Director of Vendor Risk and Compliance Services, Lynx Technology Partners, Inc.
- **Kelly Felder (Milliken)**, Enterprise Security Assessment Specialist, TSC Advantage
- **Sridhar Gundrothu**, Manager Cyber Security and Compliance, Genpact USA
- **Emily Irving**, AVP, Wellington Management, Enterprise Third Party Risk Management; Best Practices Awareness Group Chair
- **Brad Meyers**, Security Analyst
- **Brendan Murphy**, Third Party Risk & Compliance Manager, U.S. Bancorp

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

- **Bob Jones**, Senior Advisor
- **Mike Jordan**, Senior Director
- **Katherine Kneeland**, Director
- **Charlie Miller**, Senior Vice President
- **Gary Roboff**, Senior Advisor
- **Marya Roddis**, Vice President of Communications, Editor

About the Shared Assessments Program

The Shared Assessments Program is the trusted leader in third party risk management, with resources to effectively manage the critical components of the third party risk management lifecycle. Program resources are: creating efficiencies and lowering costs for all assessment 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 outsourcers. Shared Assessments offers opportunities for members to address global risk management challenges through committees, awareness groups, interest groups and special projects. For more information on Shared Assessments, please visit: *http://www.sharedassessments.org*.

Appendix 1: Glossary of Selected Third Party Risk Management (TPRM) Terms

TPRM-Related Term	Definition
Business Continuity and Resiliency (BC/BR)	Assurance that an organization's business functions will either continue to operate despite serious incidents or disasters or may otherwise recover within a pre-determined period of time.
Control Assertion Statement	A claim by an entity that specific policies, processes, controls, procedures or other mitigating techniques to reduce exposure are in place and functioning properly, as appropriate to the relationship. In "Trust, but Verify" TPRM environments, assertion statements are often third parties' responses to a set of questions typically asked by the outsourcer or its agent.
Control Objectives	A series of statements made by an organization, which: 1) provide a specific target for control evaluation; and 2) define the processes, policies and procedures in place in the organization's control environment.
Critical Third Party Service Provider	A service provider that is so vital that the incapacity or unavailability of such may have a debilitating impact on the business. Examples of industry specific guidelines include: • FFIEC Supervision of TSP – Booklet, Division of Technology. • OCC Bulletin 2013-29. OCC has a specific definition of this term that includes payments, significant shared services, major impact on operations.
Degree of Assurance	The confidence level required to be certain that a set of controls is actually in place and functioning as claimed.
Due Diligence Process	The investigative process by which a company or other third party is reviewed to determine its suitability for a given task. Due diligence is an ongoing activity, including review, monitoring, and management communication over the entire vendor lifecycle. ISACA, 2018.
Disaster Recovery (DR)	The process, policies and procedures related to preparing for and executing recovery or continuation of organization-critical infrastructure in the event of a natural or manmade disaster. Disaster recovery is a subset of business continuity and resiliency. Disaster recovery may include the process of resuming technical operations at a back-up site while recovering operations at the primary site.
Exit Strategy	Predetermined process or requirements for terminating a third party relationship. Best practice termination requirements include: return of the work product; return or destruction of data; proof of destruction and/or return of intellectual property (IP), work product and data; transition assistance; reporting requirements; insurance requirements; notification/consent to subcontracting; right to solicit/hire vendor employees; and indemnification regarding responsibility for costs and where liability lies. If the relationship involves processing that is critical, establish parallel services.
Incident Event and Communication Management	The activities of an organization to identify, analyze and correct issues and to prevent re-occurrence. Within structured organizations, these issues are normally dealt with, communicated and corrective action is taken by either an Incident Response Team (IRT) or an Incident Management Team (IMT).
Incident Response Plan	A predetermined, systematic and documented method for an organization to identify, analyze, respond to and correct issues and to prevent a future re-occurrence.
Inherent Risk	The risk level or exposure that exists before any actions (e.g., implementing controls) are taken, or might be taken, to mitigate the risk.
Key Control Indicators (KCI)	Metrics used to provide an early signal of increasing risk exposure.
Key Performance Indicators (KPI)	Indicators that measure specific goals or targets, in conjunction with the Service Level Agreement (SLA). KPIs can be Key Control Indicators (KCIs), Key Risk Indicators (KRIs), etc.
Key Risk Indicators (KRI)	Metrics that organizations can use to determine early warning on risks that may affect the enterprise. They are a primary predictor of possible future impacts.

TPRM-Related Term	Definition
Lines of Defense	A concept suggesting that organizations can best defend against risk by organizing enterprise risk management (and its subcomponents) into a structure that demonstrates precise management roles, internal compliance and control functions and audit. The structure consists of: • Business operations; • Risk and control functions; and • Internal audit. Some sources suggest that an organization's Governing Board should be considered to have an active role in lines of defense. Some observers view as part of the audit line of defense, others have proposed as a fourth line.
Mitigation	A risk control process to lessen or resolve the impact of a control weakness.
Objectives and Key Results (OKR) Indicators	A framework for defining and tracking organizational and team objectives and their outcomes, typically to provide a means of aligning and focusing efforts across an enterprise.
Onboarding	The process of integrating a new vendor into an organization. Onboarding occurs after the vendor has been selected.
Operational Risk	Operational Risk occurs when either a service provider or the outsourcer exposes an organization to direct or indirect losses due to inadequate or failed internal processes or systems. Adapted from: US Federal Reserve. https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf
Remediation	The process by which organizations address control deficiencies and maturity gaps to ensure that deficiencies are appropriately corrected, and gaps closed. In an information systems environment, remediation addresses control deficiencies.
Residual Risk	The remaining risk after management has implemented a risk response. ISACA, 2017
Risk Appetite/Risk Appetite Statement	a) Risk Appetite: The level and type of risk an organization will take in order to pursue its strategic objectives. b) Risk Appetite Statement: A documented definition of the organization's risk appetite.
Risk Appetite Framework	The core instrument for defining and aligning risk sensitivity and metrics in a specific business context across an organization. The Risk Appetite Framework operates at all levels of the organization (Board, C-Suite, Business Unit, etc.) and must include an effective risk infrastructure that integrates the organization's strategy using key metrics that tie risk to business objectives for driving and evaluating TPRM program effectiveness. The framework should incorporate the roles and responsibilities and the implementation of various risk management tools and documentation of risk policies. Actionable risk tolerance metrics must be included. Adapted from James Lam, 2017.
Risk Assessment	The process of collecting information related to and analyzing the potential impacts on its business operations that an organization may encounter.
Risk Domains	Risk Domains are categories (or areas) of risks. Shared Assessments identifies 18 third party risk domains: risk assessment and treatment; security policy; organizational security; asset and information management; human resources security; physical and environmental security; operations management; access control; application security; incident event and communications management; business resiliency; compliance; end users device security; network security; privacy; threat management; server security; and cloud hosting.
Risk Rating	*v.* A rank order quantification using a systematic approach that quantifies risk in terms of loss potential, then sequences individual risks to determine the order in which compensating controls should be implemented. When activities are outsourced, this scoring procedure also determines how often and how thoroughly third party controls and related processes (such as disaster recovery testing) are examined and tested. *n.* A value derived from assessing and prioritizing the severity of risks. Adapted from: COSO ERM, June 2017.
Risk Tiering	Assessing risk of a particular function or third party and determining across a ranked scale (e.g., 1-5, high to low). May be individually custom defined or developed by/for the organization to help understand the requirements for due diligence on an individual third party.

TPRM-Related Term	Definition
Risk Tolerance	"The quantitative thresholds that allocate the organization's risk appetite to specific risks types, business units, product and customer segments, and other levels… Risk tolerance is often used as a synonym to Risk Appetite but is quite different in practice. Certain risk tolerance are policy limits that should not be exceeded except under extraordinary circumstances (hard limits) while other RTs are guideposts or trigger points for risk reviews or mitigation (soft limits). Whereas risk appetite is a strategic determination based on long-term objectives, risk tolerance is seen as a tactical readiness to bear a specific risk within established parameters." James Lam, 2017.
Service Level Agreement (SLA)	An agreement, that is part of a service contract, which precisely defines the quality of service the customer should expect expressed as metrics. SLAs detail the responsibilities of service providers and typically detail the consequences (financial penalties, etc.) if service providers do not meet threshold expectations.
Third Party	All entities or persons that work on behalf of an organization but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person. A subcontractor may be a sub-processors or sub-service organizations when it is an entity that works for the outsourcer's third party, e.g., Service Provider contracted storage or transport services, Cloud Service providers, Disaster Recovery (DR)/Business Continuity Plan (BCP) location, contractors etc.
"Trust, but Verify" Model of Third Party Risk Management	The "Trust, but Verify" model has become the gold standard process in third party assessments. The "Trust" component of the model is typically facilitated through a query instrument (e.g., a questionnaire), a means by which the outsourcer can obtain the third party's statement about its control environment, at a detailed level if desired. The "Verify" component of the model has two primary parts which are interrelated: 1) Initial Onsite/Virtual Assessments; and 2) Ongoing Monitoring. Ongoing Monitoring, in turn, has two component parts: a) Periodic Ongoing Monitoring; and b) Continuous Monitoring.
Vendor Risk Management	The process of analyzing and controlling risks presented to an organization, its data, operations and/or finances by parties other than your own organization. Adapted from ISACA, 2017.

Appendix 2: Shared Assessments Standardized Information Gathering (SIG) Questionnaire & Standardized Control Assessment (SCA) Procedures Risk Domains

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

Appendix 3: Emerging Best Practices in Contract Due Diligence

Emerging practices in contract management, which are proving successful in moving the needle on third party risk management[xvii] include a defined organizational structure for third party contract drafting, negotiation and approval, as well as established procedures for contract exception review. The outsourcer should establish and maintain:

- Standards for mandatory contract language and provisions. Set corporate-level provision requirements, relationship termination procedures and business resiliency and security/IT provisions.
- A process to facilitate approval of final contract terms by Legal and an appropriate level of management.
- Procedures for review of existing contracts for compliance with current contract standards, with remediation processes for correcting deficiencies relative to current contract processes.
- A third party provider risk classification structure that is aligned with provider risk and ensures inclusion of appropriate, measurable performance-based indicators based on that risk within the contract provisions.
- A standardized process document, which details the contract processes and procedures within the context of planning and implementation of a third party risk management program.
- Accurate third party, product/service, inventory that provides access by internal resources to a repository which contains the Legal Name of the contracted entity on the contract along with information that can be leveraged for contract management purposes. The inventory helps to define from a monitoring perspective what has changed over time, what is open to negotiation or arbitration, and what is not.
- Alerts or other tracking system within the inventory for expiry dates of contracts and other review cycle triggers.
- Documented relationship management guidelines that include the best practice of periodically (at risk-based frequency) reviewing contracts to confirm existing provisions and update against any changes.
- Periodic reviews based on type and criticality of services and reviews triggered by pre-determined criteria, such as changes in services or locations, testing SLAs and reporting requirements.
- Maintain a Third Party Oversight Program, with defined responsibilities reducing the time Contract Management spends on ancillary items such as SLAs, Financial Review and Regulatory Alerts.
- Add a GRC tool, where feasible, for alerting and tracking and requests for documentation.
- Pre-defined standard contract language that allows for addendums, so that they can be examined, negotiated, and utilized where needed, without opening the entire contract process to renegotiation.
- Defined standard contract language for future addendums – this will create efficiency in the time it can take for the addendum to be examined, negotiated and utilized where/when necessary eliminating the review of the entire contract.

- Business planning requirements that are reviewed not only from the cyber security perspective, but also from BCP/service disruption/disaster declaration perspectives, including SLAs, such as: RTOs (Recovery Time Objectives), RPOs (Recovery Point Objectives) and Recovery Capacity, especially when multiple services are provided by the third party with differences in operational, financial, regulatory, reputation impacts.
- Defined milestones and issues identification processes for negotiation to create efficiencies:
    - Both the outsourcer and provider need time to absorb any proposed changes. If issues cannot be remediated, the contract has to allow for time to step away from the relationship, without disruption to services/infrastructure for the outsourcer or to income streams for the provider.
    - Fourth and other 'down stream' party clauses and provisions are easier to deal with in new contract negotiations than in existing contract situations.
- Internal best practices in collaboration with counsel and use that opportunity to build contract templates and policies - this will allow for addendums and security remediation covenants:
    - Determine what works best in an addendum and what works best in a contract.
    - This is a visionary stakeholder conversation, in which the third party risk practitioner and the legal department can learn from one another what works best in practical settings.
    - Define who is responsible for making these types of contract calls, what stakeholders need to be involved and/or notified and put that into an actionable policy.
- Playbooks around contract terms:
    - This provides actionable, practical guidance for internal relationships that cede their responsibilities to various subject matter expert areas (e.g., CIO and Legal Counsel can work together) for the benefit of the contract being effective.
    - Playbooks can be used to show what a contract should include, as well as options for situation-specific guidance regarding where such elements as security or social responsibility terminology would lie within the contract or addendum.
    - Standards may be third party specific (i.e., use the existing security or other risk control standard within a third party's organization as the agreed upon guideline) if that standard meets the outsourcer's risk appetite and tolerance needs.
    - Another alternative is to document best or leading practices in which a particular standard is chosen as a starting point for contract development.

Appendix 4: Sample Third Party Selection Criteria

Review Area	Sample Review Criteria	Techniques
Third Party Selection	• Are all parties that touch sensitive data identified and a risk assessment performed prior to gaining access? This includes call and data centers, as well as other outsourced service providers. • Are all parties that are consumer facing (direct contact, mail/email or systems) identified and a risk assessment performed prior to gaining access to the outsourcer's customers? • Is a system in place that is aligned with a documented risk rating and assessment process for all down stream parties? • Is an action plan in place for remediation? • Do contracts define roles and responsibilities, including monitoring of specific risk factors that are mission-critical and compliant with regulations? • Are all of the outsourcer's mission critical third parties with fourth parties identified and risk assessed during the third party selection phase? • Is the outsourcer able to identify if data resides in the cloud (private/public) and risk assessed during the third party selection and ongoing monitoring phases? • Clauses should include distinction between audit and assessment, to ensure all parties understand the right to audit/investigate/assess and the number of each type of audit, investigation or assessments that may take place over specified time periods.	• Fourth party SLAs or contract template(s) that include requirements of a risk management program comparable to the outsourcer's third party risk area requirements. • Automated collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulge fourth party relationships, even if the third party provider has not divulged those to the outsourcer. • Security Information and Event Management (SIEM) documentation demonstrating follow through of reported material event(s).

Appendix 5: Sample Monitoring Criteria for Existing and Evergreen Contracts

Review Area	Sample Review Criteria	Techniques
Monitoring	• Is there documentation of fourth parties that a third party provider has changed or newly contracted with since the last assessment report? • What is the third party's continuous monitoring process, and what is their SLA commitment to do so? • Evaluate whether the third party has the people, processes and technology in place to fulfill scoped requirements. • Determine if third party insurance is appropriate to outsourcing need. • Define roles and responsibilities. • Identify incident coordinator/quarterback and backup coordinator protocol. • Identify Point of Contact (POC) for data owner: IT/Legal/ Communications. • Outsourcing company should be notifying party. • Evergreen contracts with critical providers may inhibit the renegotiation process when negotiations need to take place to add important new risk control requirements, as one party may perceive a loss of advantage or position on non-risk elements (e.g., pricing and billing).	• Defined escalation triggers. • Additional monitoring techniques for fourth parties that support specific services (e.g., consumer facing fourth party customer complaint policies; mission critical third party participation in fourth party disaster recovery exercises; data processor adverse event policies).

Appendix 6: Sample Renewal Update or Termination Criteria

Review Area	Sample Review Criteria	Techniques
Updates and/or Termination	• Do legacy resource issues exist, such as: o Adding critical clauses to existing relationships where contracts are in place, such as right to audit, notification of use of and/or changes in fourth parties. o Possible constraints that may limit the use of addendums when risk profiles, factors, or other critical elements affecting a relationship change. • Changes to governing law or monitoring triggers may mandate control changes that are not in standard contract provisions and may be hard to implement when ongoing monitoring reveals the need to do so.	• Established playbooks that guide agile decision making when revising contracts at the third and nth party levels. • Dynamic updates to playbooks and other documentation and inventories that assist business units, Procurement and Legal in determining appropriate steps for existing, renewal and terminated relationships based on actual performance and termination data.

Appendix 7: Sample Merger and Acquisition (M&A) Contract Considerations

Review Area	Sample Review Criteria	Techniques
Mergers and Acquisitions	• Service/product continuance or notification of termination clauses in the event of a merger or acquisition. • Business continuity plan tied to outsourcer needs.	• Include clauses that allow for a pre-determined path in the event of a merger or acquisition (from either the outsourcer or the provider viewpoint). • Agreement assignment (provisions for the sale or discontinuance of business by either party etc.).

Appendix 8: Third Party Contract Development Guideline Tool by Lifecycle Stage

This table contains specific suggestions that can be used to build out organization-appropriate contract provisions and clauses to help tailor its contract templates. The table has been compiled by third party risk management practitioners to reflect best practices for developing actionable contracts. Organizations can use the guidelines to add dimension to their planning processes to optimize the critical role contract development should play in managing third party risk. This is not an exhaustive list but one that should be expanded upon by each organization based on its unique risk and service scope priorities. Each organization should evaluate the process of developing contract templates and other contract documents from its own standpoint, based on their individual organization's needs.

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Pre-onboarding Examination; Contract Development & Negotiations	• Specify a clear and complete definition of the services provided and role of the parties. • Define the duration, nature and purpose of services and products, including the delivery model, types and use of data and any allowable use of fourth parties. • Identify who owns and is responsible/accountable for contract and asset ownership. • Specify data access by location and number of personnel. Require the use of appropriate encryption (at rest and in transit). • Define and document key concepts and parameters appropriate to the outsourced activity: e.g., data types, uses, allowed access and retention parameters; *Electronic Discovery Reference Model (EDRM)* requirements for legal discovery orders (length of retention, preservation of records); protection of sensitive information. • Define and document appropriate policies, procedures and technology are in place to engage, monitor and evaluate providers and conduct other activities that may be required, such as EDRM. • Ensure the inclusion of monitoring requirements and reporting thresholds that are appropriate to the risk and relationship, which may include Security Information and Event Management (SIEM) documentation demonstrating follow through on any material event(s). • Require fourth party SLAs to include right of Outsourcer to conduct security assessments on third party's subcontractors.	• ***Establish third party contract management processes aligned with industry best practices.*** • ***Establish criteria for the alignment of contract provisions with third party risk classification structure. Consider risk scoring the provider at the contract service component level.*** • Set guidelines based on requirements, based on: o The business unit's requirements for the third party; o The technical requirements (e.g., data elements, IT components, connectivity); and o Define any third party specific requirements for their outsourcer(s). • Determine and document: o Ownership, roles and responsibilities that are clearly defined and enforced. o Who owns the data or other assets that are handled within the contract. o What controls are in place. o Is there litigation in process that names the organization or its key personnel? o Is there financial data that indicates potential changes in risk vulnerabilities? o Is there evidence of changes to core mission, business processes or enterprise architecture?

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Pre-onboarding Examination; Contract Development & Negotiations	• Distinguish between audit and assessment, to ensure all parties understand the types and rights to receive reports on subcontractor performance, compliance, etc. – including audit, assessment and investigative reports. o Include a right to audit clause that provides the outsourcer with the following rights: • Ability to perform due diligence (see Appendix 1: Glossary); • Periodic refresh of due diligence; • Artifacts that need to be provided in support of attestation of controls and onsite reviews (e.g., reports, data flow charts, etc.). o Define the number of each type of audit or assessment that may take place over specified time periods, with minimum annual assessment allowance and parameters for ongoing and continuous monitoring that are tied to the level of risk posed by that provider. o Define an annual assessment allowance and parameters for ongoing and continuous monitoring that are tied to the level of risk posed by that provider." o Include a "right to investigate" clause to ensure satisfactory due diligence after a significant security event at third parties or subcontractors. Contract language to allow the outsourcer to have access to forensic investigations conducted on the third party on behalf of the third party or outsourcer. • Require timely notification of disruptive events, with definition of what those types of events are for a given provider. • Ensure the third party's liability for action/inactions of its subcontractors, also including the third party's responsibility for the costs and resources required for additional monitoring and management of its subcontractors.	o Which party is responsible for cybersecurity insurance and/or costs associated with investigation and/or damages? o Has a variant or trade name been edited into the contract during signing or prep stages? o Escalation processes should be tied to industry standards. o Understand vendor's standard contract needs. o Promote information sharing. • Regarding incident management: o Be proactive on both vendor and outsourcing organization sides re: forensics investigations. o Develop standard of who/when/how soon to notify, including backup protocol and information required. o Determine what Scribe/Tool rules will be used. o Establish an investigation playbook. • Review business resiliency planning not only from the cyber security perspective, but also from Business Continuity Planning/Service Disruption/Disaster Declaration Perspectives, including SLAs, such as: Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and Recovery Capacity especially when multiple services are provided the third party with differing operational, financial, regulatory, reputation impacts. If services are not delivered within defined SLAs.

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Pre-onboarding Examination; Contract Development & Negotiations	• Include a right to terminate the contract without penalty if a third party's subcontracting practices or arrangements do not comply with the terms of the contract. • Require third party to provide notification to and/or receive approval from outsourcer prior to the third party's use and/or change in fourth party providers. • Require fourth party SLAs to include a risk management program comparable to the outsourcer's third party risk area requirements, or include contract template clauses that mandate such requirements. • Specify all parties with access to sensitive data, including call and data centers, and any other outsourced service providers. • Through the use of applicable provisions, ensure the contract conforms and/or complies with current regulations pertinent to the relationship and geolocation of service provision or location of the provider (e.g., GPDR, China Cybersecurity Law, New York State Department of Financial Services cybersecurity regulation 23 NY CRR500). • "Use clear definition(s) and understanding(s) regarding compliance (such as GDPR and handling of private information), including: o Compliance with applicable laws and regulations. o For international transfers of Personal Data from the EU, specify the legitimizing method utilized: e.g., model contracts/clauses, binding corporate rules, Privacy Shield, adequate country designation. • Ensure contract includes: o Full legal name of the contracted entity on the contract. o Service Oriented Architecture (SOAs). o 24x7 Service Level Agreement(s), specific for failure to comply. Define consequences of failure to perform (including penalties/termination). o Security Remediation Covenant(s).	• Consider: o Are all parties that are consumer facing (direct contact, mail/email or systems) identified and a risk assessment performed prior to gaining access to the outsourcer's consumer customers? o Is an action plan in place for remediation? o Do contracts define roles and responsibilities, including monitoring of specific risk factors that are mission-critical and compliant with regulations? o Are all of the outsourcer's mission critical third parties with fourth parties identified and risk assessed during the third party selection phase? o Are all of the outsourcers able to identify if data resides in the cloud (private/public) and risk assessed during the third party selection and ongoing monitoring phases?

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Pre-onboarding Examination; Contract Development & Negotiations	o Legal representation. o Event notification – Security and/or data breach notification and resolution process. Vendors MUST notify by issue type and specify time frame. Clearly defined escalation processes that are tied to pre-determined (documented at a point in time) industry standards. Indemnification regarding responsibility for costs and where liability lies. o Service/product continuance or notification of termination clauses in the event of a merger or acquisition. o Business continuity plan tied to outsourcer needs. o Clearly defined escalation processes. o "Per GDPR requirements, contracts should include provisions that imposes on the third party and/or their subcontractors: • A Code of Ethics containing a Privacy Section; and • A Privacy Training Program, with evidence required of training and certification for each individual with access to private data. o Require written documentation on data repositories, data flows, and data processing. The contract should also include definitions of specific limitations on data access, including geolocation and security of data (e.g. maintained offshore or onshore, whether encrypted in transit and/or at rest), as applicable. o Include insurance and reporting requirements for third parties and/or subcontractors. Depending on the situation, the reporting requirements could be service or performance related documentation and/or financial statements. o Include Information Security and Confidentiality requirements, with cybersecurity assurances, such as cyber insurance, where appropriate.	

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Pre-onboarding Examination; Contract Development & Negotiations	• Include a Business Continuity Plan (BCP) that is tailored to address the Outsourcer's needs. • Include provision to provide outsourcer with prior notification of material changes to a third party's risk profile, including security program and data protection protocols. • Provisions covering the assignment of the contract to successors in interest (in cases of the sale of or discontinuance of business by either party, etc.). • Include a well-defined exit strategy - Termination conditions, as well as process of termination (who owns the work product, return or destruction of data etc.). Contract termination requirements, including proof of destruction and/or return of intellectual property (IP), work product and data. If the processing is critical, establish parallel services. Transition assistance, reporting requirements, insurance requirements, notification/consent to subcontracting, right to solicit/hire vendor employees. Indemnification regarding responsibility for costs and where liability lies.	

EXISTING RELATIONSHIPS & EVERGREEN CONTRACTS

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Vendor Relationship Management (VRM)– Ongoing Monitoring and Reviews of Existing Relationships	• Define and document periods (cycles) for reviews and updates, as needed, to Master Services Agreements ensures both parties are aware of changes in third party processes or other organizational considerations that may mandate changes to the contract and/or addendum. • Define and documentation process for escalation triggers. • Include additional monitoring techniques for fourth parties that support specific services, such as: o Consumer facing fourth party customer complaint policies; o Mission critical third party participation in fourth party disaster recovery exercises; and o Data processor adverse event policies. • Examine and catalog processes that are outsourced. • Clarify the nature and value of specific relationships. • Examine existing clauses to: o Ensure that clauses and/or provisions still meet outsourcer risk profile needs. o Document changes to services, products, criticality since an original contract was executed. • Determine and document if cyber insurance an effective part of the organization's risk management program (financial institutions specifically). • To cover the possibility of a merger or acquisition, include provisions that address service and/or product continuance or notification of termination clauses.	• Establish vendor relationship management processes aligned with industry best practices. • Maintain as consistent a third party support team as possible. • Educate third parties on required roles and responsibilities for nth party contractors. • Management of key third party risk operational points: o Sourcing and third party management team coordination; o Organization-appropriate third party risk classification; o Monitoring of third party performance; o Effective use of assessment results; and o Prompt response to and management of any third party performance issues, as they arise.

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Vendor Relationship Management (VRM)– Ongoing Monitoring and Reviews of Existing Relationships		• Over the review period, document: o Is there documentation of fourth parties that a third party provider has changed or newly contracted with since the last assessment report? o What is the third party's continuous monitoring process, and what is their SLA commitment to do so? o Targeted collection (automated) of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulge fourth party relationships, even if the third party provider has not divulged those to the outsourcer. o Is there litigation in process that names the organization or its key personnel? o Is there financial data that indicates potential changes in risk vulnerabilities? o Is there evidence of changes to core mission, business processes or enterprise architecture? o Does the third party meet its agreed upon schedule for security status reporting to the outsourcer (e.g., annual/semi-annual/quarterly)?

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Vendor Relationship Management (VRM)– Ongoing Monitoring and Reviews of Existing Relationships		o Documentation of fourth parties that a vendor has changed or newly contracted with since the last assessment report? o Are there unauthorized components or other risk vectors present, such as: improperly configured Sender Policy Framework (SPF) configurations; expired Secure Socket Layer (SSL) certificates; missing or altered application security headers; or unnecessary open ports? o Is there evidence of software patches and intrusion detection/virus prevention tool updates being applied, as needed, in a timely manner? o Is your vendor aware of and do they share information about its own outsourcer satisfaction and risk profile ratings?

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Evergreen Contracts	• Examine existing clauses to: o Ensure that clauses and/or provisions still meet outsourcer risk profile needs. o Document changes to services, products, criticality since the original contract was executed. • Update contract for any required changes to regulations that require changes to contract(s) or Master Services Agreements (MSAs).	• ***Have pre-defined standard contract language that allows for addendums, so that they can be examined, negotiated, and utilized where needed, without opening the entire contract process to renegotiation.***

CONTRACT RENEWALS & TERMINATIONS		
RELATIONSHIP LIFECYCLE STAGE	**RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES**	**RELEVANT BEST PRACTICE CONSIDERATIONS**
Renewals	• Examine existing clauses to: o Identify whether terms still meet outsourcer risk profile needs. o Document changes to services, products, criticality since the original contract was executed. o Update contract for any required changes to regulations that require changes to contract(s) or Master Services Agreements (MSAs). • Determine if remediation and continuation appropriate. Escalate as needed, based on pre-agreed terms and/or outsourcer policies. • Determine if contract termination is appropriate (by cycle, by need, by cause). Escalate as needed, based on pre-agreed terms and/or outsourcer policies. • Re-examine/reassess service/product continuance or notification of termination clauses in the event of a merger or acquisition.	• ***Establish vendor review and renewal processes.*** • ***Establish pre-defined standard contract language that allows for addendums, so that they can be examined, negotiated, and utilized where needed, without opening the entire contract process to renegotiation.*** • ***Establish criteria for the re-alignment of contract provisions with vendor risk classification structure.*** • Utilize addendums when feasible to amend terms, rather than renegotiation to achieve key objectives (such as: additional monitoring, control over fourth parties, or updates required due to changes in regulations). • If termination will be by cause, document root causes: o Was the provider appropriately rated? o Did controls fail? o Are there monitoring, control logs, evidence? o Pen Testing - are they performed regularly internally and externally; at what intervals; and are they performed by credentialed Pen testers?

RELATIONSHIP LIFECYCLE STAGE	RECOMMENDED GUIDELINES ON PROVISIONS AND CLAUSES	RELEVANT BEST PRACTICE CONSIDERATIONS
Termination	• Termination that occurs by contract provision (reaches the end of the contract term). Wind down, document using a pre-defined exit strategy. • The exit strategy from the contract should be well-defined, and include: o Termination conditions, as well as the process of termination (who owns the work product, return and/or destruction of data, etc.); o Contract termination requirements, including proof of destruction and/or return of intellectual property (IP), work product and data; o If the processing is critical, establish parallel services; o Transition assistance, reporting requirements, insurance requirements, notification/consent to subcontracting, right to solicit/hire vendor employees; and o Indemnification regarding responsibility for costs and where liability lies. • Ensure there is no service disruption during the winding down period. • Implement and monitor data security components to coincide with the third party separation, and validate transfer and/or destruction of data. • Recover any and all fourth party subcontractor or licensee data. • Ensure proper notice of termination or non-renewal is sent. • Communicate timely internally about any discontinued relationships – possible "inactivation" in any vendor system – to prevent staff from using a vendor who is essentially no longer approved/ contracted.	• ***Document the termination in the vendor inventory and communicate the reason(s) for termination, so that Procurement and other business units have this information available for other existing contracts with the provider and for future reference.*** • If termination was by cause, document root causes: o Was the provider appropriately rated? o Did controls fail? o Are there monitoring, control logs, evidence?
	• Review business resiliency planning from the cyber security perspective and from Business Continuity Planning/Service Disruption/Disaster Declaration Perspectives, including SLAs, such as: o Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and Recovery Capacity, especially when multiple services are provided the third party with differing operational, financial, regulatory, reputation impacts. o Define consequences and timelines if services are not delivered within defined SLAs.	

Appendix 9: Examples of Regulations and Industry Standards Surrounding Contract Management

A few examples follow of how evolving regulations and standards are dictating changes to the ways in which contracts are managed:

- **European Union General Data Protection Regulation (GDPR):** *Any contracts including existing ones that are in place on May 25, 2018, and new ones after this date will be required to conform to the GDPR.* Prescriptions for certain matters must be stipulated in contracts or other legal engagements. It is essential to a comprehensive review of contract privacy considerations, that a complete inventory of all data controller and data processor contracts be created and maintained. Article 28 of the GDPR contains a number of items regarding contracts that are specific to roles involved in data processing. Data controller obligations under GDPR will trigger new contract provisions based on the scope of work, classification of personal data, and the types of data processor relationships. Article 24 (1), Article 29 and Article 46(1) define specific obligations for controllers that impact data processing and thus the data processor contract. Operational considerations for the processing of data and appropriate safeguards will trigger additional data protection contract provisions. Note that the Working Party (i.e., the current group of 28 countries), the EU Commission and member states are still refining their guidance and enacting local regulations in relation to GDPR. Therefore, anticipate that this regulation will be updated over time, as the parties further identify and refine their privacy concerns. The Shared Assessments GDPR Tool Kit provides background and tools and can be downloaded for free at: *https://sharedassessments.org/gdpr-tool-kit/*.

Under GDPR, contracts should also include the following terms requiring the processor to:

- Act only on the written instructions of the controller.
- Ensure that the data processor is subject to a confidentiality requirement.
- Engage only sub-processors with the prior consent of the controller and under a written contract.
- Assist the data controller in providing data subjects access and allow them to exercise their rights under the GDPR.
- Delete or return all personal data to the controller as requested at the end of the contract.
- Submit to audits and inspections.
- Provide the controller with the information it needs to ensure that they are both meeting their Article 28 obligations.
- Inform the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
- Processor to provide completed SIG Privacy Tab or similar assessment at least annually, subject to controller review and acceptance.
- Completed third party attestation such as the SCA and/or SOC 2.[xviii]
- Code of Ethics containing Privacy Section.
- Evidence and results of Code of Ethics training by each individual with access to Personal Data.
- Defined Privacy Training Program.
- Evidence and results of Privacy training by each individual with access to Personal Data.
- Written documentation on data repositories, data flows and processing.

- **China Cybersecurity Law:** China's cyber rules contain an overarching framework that includes network, product, services and operations safeguards for the protection of personal information and "national cyberspace sovereignty/security." The law applies directly to network and critical information structure operators (CII). CIIs must retain private information and key data collected or produced while operating within China. The terminology within the law is loosely defined and may apply to almost all businesses that own or administer their own network. It is essential to a comprehensive review of the rules as they apply to contract provisions regarding network operation, information security and privacy protection, monitoring and incident response, cross border data transmission, as well as security assessments and issues of national sovereignty.[xix]

- **US Regulations:** Financial services industry regulators have a number of rules that apply directly to due diligence and contract management.
  - The **Federal Financial Institutions Examinations Council (FFIEC)** Examination Handbook Appendix J specifies nine elements that should be included in contracts: (1) Right to Audit with the ability to perform due diligence, periodic refresh of due diligence, artifacts that need to be provided in support of attestation of controls and on site reviews; (2) establishing and monitoring performance standards; (3) default and termination provisions stating resilience requirements if service is disrupted vs. disaster is declared; (4) use of subcontractors with specified requirements for due diligence and sharing results; (5) use of foreign-based service providers; (6) effective business continuity planning (BCP) and testing with the ability to participate with third party service provider in collaborative testing; (7) data governance provisions; (8) TSP updates; and (9) security issues/incident notifications.[xx]
  - The **Office of the Comptroller (OCC)** 2017 rules mandate specifically that boards review and approve contracts with critical third parties, as well as the methodologies used for determining critical activities and managements plans for using third parties involved in critical activities and their summary of due diligence results.[xxi] The OCC further notes that monitoring should be included as part of the onboarding contract process, as "…without a repeatable, automated process in place that incorporates best practices, organizations cannot create sustainable vendor lifecycle management programs."[xxii]
- **Examples of Industry Standard Specific Guidelines for Contracting:**
  - The **Association of Corporate Counsel (ACC)** developed a set of model controls to help in-house counsel as they set expectations with their outside vendors, including outside counsel, regarding the types of data security controls these vendors should employ to protect their organization's confidential information. The Model Controls can be used to help build contract provisions with third parties, as it provides a list of baseline security definitions, measures and controls, such as retention, certification, encryption, data handling, physical security and incident reporting that offer in-house counsel a streamlined and consistent approach to setting expectations with respect to the data security practices of their outside vendors.[xxiii]
  - The **American Bar Association (ABA)** issued cyber-specific standards for contracting in 2016 "to assist procuring organizations, vendors and their respective counsel to address information security requirements in their transactions." The guidelines provide specific language around definitions, control expectations, testing requirements, connectivity and information privacy and the need for the outsourcers risk profile to be considered when developing provisions around data access, business continuity and regulatory compliance and/or conformity.[xxiv]
  - **US Chamber of Commerce (USCOC)** issued the Principles for Fair and Accurate Security Ratings in 2017 to provide more organizations to promote fairness in reporting and enhance the ability of businesses in all industries to leverage security ratings in making risk-based decisions. Six principles are at the heart of this approach and companies can agree to be supportive of these principles and be recognized as doing so. These principles are: Transparency; right to Dispute, Correction and Appeal; Accuracy and Validation; Model Governance; Independence; and Confidentiality.[xxv]

Appendix 10: Additional Resources

Related Best Practices Awareness Group white papers and other Shared Assessments Resources include:

- *Vendor Risk Management Benchmark Annual Survey.* Shared Assessments and Protiviti 2017 Research Study.
- *Appendix: Article 28 Contract Considerations General Data Protection Regulation (GDPR): Data Processor Privacy Tool Kit.* 2018 Program Tool and Template Set.
- *Risk Rating Third Parties: Optimizing Risk Management Outcomes.* 2017 White Paper.
- *Evaluating Cloud Risk for the Enterprise: An Updated Shared Assessments Guide.* 2017 White Paper.
- *Assessment of Public Cloud Vendors: Emerging Best Practices.* 2017 White Paper.
- *Fourth Party Risk Management: Supply Chain Issues and Emerging Best Practices.* 2017 White Paper.
- *Continuous Monitoring of Third Party Vendors: Building Best Practices.* 2017 White Paper.
- *Building Best Practices in Third Party Risk Management: Involving Procurement.* 2016 White Paper.
- *Building Best Practices for Effective Monitoring of a Third Party's Incident Event Management Program.* 2015 White Paper.

Other, industry specific guidelines for contract provisions include:

- *Cybersecurity Legal Task Force Vendor Contracting Project: Cybersecurity Checklist.* American Bar Association (ABA). November 2016.
- *FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs.* April 2018.
- *FFIEC Information Technology Examination Handbook. Appendix J: Strengthening the Resilience of Outsourced Technology Services.* FFIEC. February 2015.
- *Third-Party Relationship: Supplemental Examination Procedures Bulletin.* OCC 2017-7. January 2017.
- *Principles for Fair and Accurate Security Ratings.* US Chamber of Commerce. June 2017.