Global Third Party Risk Management Policy

Introduction

This Global Third Party Risk Management Policy (the "TPRM Policy" or the "Policy") sets forth standards regarding Crawford's engagement of outsourced or vendor supported work functions and is designed to provide a framework for Crawford to identify, measure, monitor, and report third party supplier risk.

Policy

Crawford recognizes that the aim of third party supplier risk management is not to totally eliminate risk, but rather to provide the structural means to allow Crawford to identify, prioritize, manage, mitigate or respond to the risks involved in supplier and/or partner service activities, while protecting the integrity of Crawford's brand and reputation.

Crawford & Co. ("Crawford") relies on third party relationships to:

- Perform services and provide products on its behalf; and
- Provide services and products that Crawford may not perform internally.

Using third parties reduces management's direct control of activities and may introduce new or increase existing risks, such as disruptions, delays, or other events causing a denigration of transaction processing, customer service, IT & physical security and data privacy. Detailed risk type descriptions can be found in the Glossary of Terms section of this document.

Crawford may amend this Policy and introduce new third party risk management policies and procedures.

Policy Implementation

This Policy is intended to be implemented under a phased approach, to provide for the requirements to be appropriately and effectively operationalized. In addition, due to the nature of certain contractual agreements and business relationships, existing relationships with third parties may be addressed on a renewal or other forward-looking bases.

Definition of Third Party

Crawford enters into business relationships with a variety of third parties to perform and provide services and products. For the purpose of the TPRM Policy, a "third party" includes any entity or person not under the direct business control of Crawford with whom Crawford engages in a business relationship, including any vendor, supplier, support provider, fulfilment provider, agent, consultant, advisor, contractor, business, marketing or strategic partner, joint venture, associate and correspondent. Third parties do not include Crawford employees, or Crawford clients and customers that have not entered into any business relationship with Crawford beyond their direct engagement of Crawford to provide services to the client. Third parties include any company or individual covered by one of the following descriptions:

- Provides systems, information, products, services, and professional services for the performance of specified functions or activities (e.g., vendors including business process outsourcing, technology providers, consultants, and law firms);
- Provides products or services offered directly to Crawford's clients or supports the delivery of products or services to Crawford's clients (e.g., service providers including claims management, call centers, loss mitigation, insurance monitoring and other outsource contractors and servicers);
- Actively provides customer lead or referral information to Crawford (e.g., referral partners);
- Suppliers such as brokers, appraisers, underwriters and agencies.

Objectives

Provide a framework to manage the risks associated with conducting business with third parties, including by:

Understanding the nature of Crawford's interaction with the third party and the potential impact the relationship would have on the Crawford's operations and Crawford's clients—including access to or use of those clients' confidential information, joint marketing or franchising arrangements, and handling of customer complaints.

- Establishing a global framework that formalizes processes for managing, measuring and controlling risks related to the third party management life cycle, notably onboarding; monitoring ongoing performance (including establishing and testing agreed controls and performance metrics for suppliers), compliance and agreed controls; re-assessing risk; and off-boarding;
- Identifying critical supporting activities, including a cadence of periodic risk assessments; annual policy review and update, as necessary; reporting; policy exception processes; and training.

Roles and Responsibilities

Third Party Risk Management Organization

Crawford has appointed a Vice President of Global Third Party Risk Management who is also the Policy Owner.

The Office of Enterprise Risk Management (ERM) is the governing body for overall risk activities for Crawford & Co. including third party risk management. The ERM is responsible for:

- Conveying Crawford's risk to the Board;
- Providing oversight of Crawford's management of operational

risk, such as the risks associated with doing business with third parties;

- Understanding the risks associated with third party arrangements and monitoring risk management practices on an annual basis; and

Reviewing and providing final approval of the TPRM Policy and subsequent revisions at least annually.

First Line of Defense Business Relationship Owners

Crawford business units using third parties are responsible for managing all aspects of the relationships. The head of the business unit is responsible for designating the Business Relationship Owner ("BRO") for each third party relationship.

BROs will have primary responsibility for managing third party relationships and represent the first line of defense for ensuring compliance with the TPRM Policy, including:

- Understanding and ensuring compliance with TPRM Policy requirements;
- Comprehensive understanding of the product and/or services being provided by third parties including risks and impacts to Crawford's operations;
- Attending required TPRM Policy training;
- Monitoring and reporting events that may have a material impact on the third party's ability to perform, such as regulatory compliance issues; data security incidents; changes in business continuity capabilities; and deterioration in financial condition; and Service Level Agreement ("SLA") performance against defined metrics and contractual obligations;
- Working with TPRM Policy Owner to escalate significant incidents, issues, and matters to the ERM, e.g., third parties experiencing data security incidents, severe financial deterioration, or operational disruptions.

Second Line of Defense

The TPRM Organization is the Second Line of Defense and will serve as the policy definition and governance body, supported by Subject Matter Experts ("SME") with the functional expertise needed to ensure risks associated with third parties are fully understood and managed to an acceptable risk level. These SMEs may include legal, procurement, business continuity planning, information security, finance, insurance, compliance and others.

Global Third Party Risk Management Policy

TPRM Policy Owner

The TPRM Policy Owner will provide TPRM Policy direction and coordination across Crawford, such as:

- Overseeing the design, implementation, execution, and effectiveness of the TPRM Policy and recommending approval of the TPRM Policy and subsequent revisions to ERM;
- Establishing a consistent metric-driven inherent risk-tiering of all third parties;
- Developing a schedule for risk assessments and periodic re-assessments;
- Tracking and monitor TPRM policy exceptions and provide periodic reports as required;
- Investigating identified and reported violations.

Global Procurement

Global Procurement responsibilities may include:

- Establishing regular reporting, including maintaining a list of active third party relationships and relevant performance and compliance metrics;
- Understanding under the direction of the legal department the types of third parties who need contracts and those who don't;
- Ensuring third parties provide competitive pricing;
- Assisting business units in determining detailed sourcing requirements;
- Distributing RFIs/RFPs and review responses; and
- Working with BROs throughout the contract negotiation process to ensure relevant risks are adequately addressed in each contract and third party agreement.

Legal

Legal third party risk management activities may include: Ensuring contracts clearly state the duties, obligations, contingencies, and responsibilities of third parties and the obligation to maintain adequate internal controls, such as:

- Setting measurable Service Level Agreement(SLA) performance metrics that define the expectations and responsibilities for both parties including conformance with regulatory standards or rules;
- Responsibilities for providing, receiving, retaining and disposal of information;
- The right to audit and require remediation;

- Ownership and license;
- Supplier/servicer confidentiality and integrity;
- Business resumption and contingency plans;
- Stipulate when and how the third party should notify Crawford of its intent to use a subcontractor, subject to Crawford approval.

Subject Matter Experts ("SME's")

Subject Matter Experts (SMEs) are individuals or teams with the requisite expertise to assess risks for a particular functional area and supporting the TPRM Organization in assessing risks and controls, proposed remediation plans and providing guidance to the BROs. These activities may include in part conducting privacy impact assessments, conferring with legal on privacy and data security contract terms, and conducting sanctions screening. SMEs may include representatives from finance, privacy, information security, insurance, business continuity planning, compliance, legal and others.

Third Line of Defense – Audit

As the Third Line of Defense, Audit provides a retrospective review for compliance with the TPRM policy.

Risk Assessment and Processes

Risk Rating Framework

A risk rating should be applied to each vendor relationship based on the criticality of the products/services provided and the manner in which they are provided. The risk rating should be used to determine the scope and depth of the due diligence performed, documentation requirements, contractual terms and conditions, the scope, depth, and frequency of monitoring and risk re-assessments, and the transition process for off-boarding. Third Parties performing multiple services for Crawford should be managed following the highest tier of risk based on the breadth of services being performed.

Tier 1:

Any third party that in order to provides its services to Crawford, or on a regular basis as part of the services it provides Crawford, regularly receives or has access to **Confidential Information** as defined under the Crawford Global Data Classification Policy, or data which depicts or is reasonably understood to represent Crawford's competitive advantage will be ranked as Tier 1. Additionally, any third party whose services are unique or critical to Crawford's business or where there is a limited pool of qualified third parties to select from will be ranked as Tier 1. These third parties are deemed **high** risk to Crawford.

Tier 2:

Any third party that has access to proprietary or other internal information will be

ranked Tier 2. Based on their services, these third parties are deemed **moderate** risk to Crawford.

Tier 3:

Any third party that does not have access to Confidential Information, proprietary or other sensitive information. Third parties that have access to publically available information and additionally, any third party that performs services that do not materially affect Crawford's operations may be ranked as Tier 3. These third parties are deemed **low** risk to Crawford.

The scope of the third party risk assessment should be scaled based upon the criticality, complexity and risk of business functions or services.

An illustrative example of supplier risk and attributes is provided below.

Tier 1 – Highest Risk Tier	**Tier 2 – Moderate Risk Tier**	**Tier 3 – Lowest Risk Tier**
Attributes: • Supports critical business functions • Requires access to PII/PHI for service • Represents core risk to Crawford's services should they fail	Attributes: • Support essential business functions • Usually does not have access to PII/PHI • Represents moderate risk to Crawford's services should they fail	Attributes: • Services are not critical; easily replaced • Does not have access to PII/PHI or confidential data; only public info • Represents low to no risk to Crawford's services should they fail
Examples: • Claims Management Provider • Data Center/Hosting Provider • Business Process Outsourcing	Examples: • Software development providers • Marketing partner • Independent contractor service providers	Examples: • Office supply provider • Occasional services (e.g. catering, repairs)

Due Diligence Requirements

Due diligence should be conducted on all potential third parties before selecting and entering into contracts or relationships. Prior experience and/or knowledge of

the third party is not an acceptable proxy for due diligence. A standardized risk assessment will be leveraged to assess the criticality and/or sensitivity of services provided by the third party. The results of the risk assessment questionnaire should dictate the level of due diligence required.

The degree of due diligence should be commensurate with the level of risk and complexity of the third party relationship. More extensive due diligence should be performed when a third party relationship involves critical activities; with the option of on-site visits conducted to fully understand the third party's operations, capacity and understand and assess risk. If information is uncovered that warrants additional scrutiny the scope or assessment methods of the due diligence shall be expanded appropriately.

The following factors shall be considered as part of due diligence processes at minimum:

- Overall financial condition and viability;
- Compliance with legal, regulatory, and industry requirements;
- Adequacy of internal controls including privacy, information and physical security controls;
- Ability to comply with service level performance commitments to Crawford;
- Adequacy of the third party's business continuity planning and capabilities;
- Adequacy of the third party's governance program over secondary (4th party) suppliers.

If client information or sensitive Crawford information is shared with the third party, information security controls that specifically address use, applicable laws, regulations, industry requirements, or other identified physical and information security risks and background check requirements must be included in the contract.

Contract approval is subject to Crawford's then current approval processes.

Other Policy Considerations

Oversight and Performance Monitoring Requirements

Third parties that enter into a contract with Crawford and are determined to be risk rated Tier 1 or Tier 2 shall be subject to oversight and performance monitoring.

The objective of the oversight and performance monitoring requirements is to identify actual risks, emerging risks, and deterioration in performance early in order to facilitate timely corrective action.

The Business Relationship Owner (BRO) should keep senior management apprised of the overall health of the third party relationships and flag and escalate significant issues or concerns identified during monitoring. Examples of the type of issues include deterioration in financial condition, missed service levels, security

breaches, data loss, service or system interruptions, or compliance lapses.

Third Party Risk Re-Assessments Requirements

Third parties risk rated Tier 1 and Tier 2 are subject to a periodic risk re-assessment as defined in the risk re-assessment schedule or more frequently if the nature of the business relationship and/or criticality of services provided materially changes. Tier 3 third parties are subject to re-assessment with material changes in services, supplier relationship.

The purpose of the re-assessment is to determine any changes to the supplied services that may result in the risk rating change, which may in turn require revisions to the monitoring and re-assessment scope and frequency and contractual terms and conditions.

Risk Re-Assessment Schedule

Based upon the criticality of the services provided by a third party a risk re-assessment schedule must be developed and implemented. Similar to the due diligence process, risk re-assessment may be supplemented by an onsite visit.

The third party's risk rating determines the type of re-assessment work conducted, with TPRM Organization using the following schedule:

Risk Rating	Risk Re-Assessment
Tier 1 - Strategic / High Risk	Annually
Tier 2 – Medium Risk	Bi-annually
Tier 3 - Low Risk	Initial assessment, re-assessment with material changes in services, supplier relationship

Third Party Off-Boarding

Within the TPRM framework, procedures will be developed for the off-boarding of 3rd party suppliers.

Third party off-boarding may occur when a third party contract or relationship expires or is terminated for any reason.

In all cases, regardless of the underlying cause, all contract terminations require BROs to review the action with legal, compliance, information security, procurement and others as required prior to formalizing the contract termination.

Special attention shall be given require data return or certified destruction.

Succession Plans

As a precaution to an unexpected or sudden termination, each third party

relationship risk rated as Tier 1 and providing critical business services or supporting critical business functions should have and maintain a succession plan designed to provide continuation of the critical services in the event of discontinuation of such services by the incumbent supplier.

Annual Risk Assessment

The TPRM Policy Owner will conduct an annual policy review of Crawford's TPRM Policy and related processes and programs to determine the effectiveness of the policy and implementation. The risk assessment shall validate whether the TPRM Policy is aligned with applicable legal, regulatory, and industry requirements.

Policy Exceptions

A "policy exception" is any deviation from the TPRM Policy. Policy exceptions are generally discouraged; however, policy exceptions require TPRM Policy Owner approval. The status of policy exceptions shall be tracked and reported upon periodically until closed.

Policy Violations

Failure to comply with the TPRM Policy may adversely affect Crawford's business and stakeholders and increase the level of risk to the organization.

Additionally, it is the responsibility of all personnel to report violations of or non-compliance with the TPRM Policy to TPRM Policy Owner immediately.

Personnel found violating the TPRM Policy may be subject to disciplinary action up to and including termination of employment.

Training and Awareness

Training should be performed for all personnel with a role or responsibility requiring an awareness and understanding of the TPRM Policy. The objective will be to reinforce individual accountability and elevate the overall effectiveness of TPRM Policy implementation and execution.

Policy Owner

The Vice President of Third Party Risk Management is the "owner" and responsible for updating and maintaining the Global Third Party Risk Management Policy.

Governance

The Policy Owner is the Vice President of Third Party Risk Management, responsible and accountable for the maintenance, implementation, interpretation, and management of the TPRM Policy and to ensure related programs and processes are effective and coordinated with all stakeholders.

Governance and oversight for the TPRM Policy will be follows:

- The Office of Enterprise Risk Management (ERM) is responsible for reviewing and approving the TPRM Policy and subsequent revisions; and
- The TPRM Policy Owner is responsible for overseeing the design, implementation, execution, and effectiveness of the TPRM Policy and recommending approval of the TPRM Policy and subsequent revisions to the ERM.
- Proper documentation and reporting must be maintained to facilitate the accountability, monitoring, and risk management associated with third parties and will include the following at minimum:
- Current inventory of all third party relationships which clearly identifies those relationships that involve critical and/or sensitive business activities and identifies the risks posed by those relationships across the Company
- Risk schema and supplier tiering or classification models
- Due diligence results, findings, and recommendations
- Executed contracts fully describing the products or services to be provided and the rights of the parties
- Regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements
- Regular reports to the board and senior management on the results of internal or external reviews of the Company's overall risk management process
- Retention requirements for third party supplier risk history and associated documentation.

Periodic independent reviews should be conducted of the third party risk management process, particularly when the Company involves third parties in critical business activities. Reviews should include assessing the adequacy of the Company's processes and third party relationship alignment with the Crawford's business strategy.

- Responding to material breaches, service disruptions, or other material issues
- Identify and manage risks associated with complex third party relationships, including foreign-based third parties and subcontractors
- Involve multiple disciplines across the Company as appropriate

during each phase of the third party risk management life cycle

- Oversight and accountability for managing third party relationships (e.g., where roles and responsibilities are clearly defined and assigned and where the individuals possess the requisite expertise, resources, and authority)
- Appropriate controls exist to ensure conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties

Identify and manage concentration risks that may arise from relying on a single third party for multiple activities, or from geographic concentration of business due to either direct contracting or subcontracting agreements to the same locations.

Scope

The Global Third Party Risk Management (TPRM) Policy is applicable to all Crawford third party relationships, and the engagement with any Third Party by employees, contractors, and temporary staff of Crawford (collectively, "personnel"). In this Policy, "Crawford" includes all majority-owned or controlled subsidiaries of Crawford & Company.

This Policy excludes any third party relationships with taxing jurisdictions. Where dual relationships with Crawford exist, such as where a third party is both a client and a supplier, the TPRM Policy Owner shall have responsibility for determining policy applicability.

Contact

For more information on this policy, contact the Third Party Risk Management Program Owner.

Document Information

Document Name	Global Third Party Risk Management Policy
Category	Global Policy
Related Policies	This policy is to be read and applied in conjunction with the Crawford's documented procedures and other applicable policies, including, but not limited to: • Information Security Policy • Privacy Policy • Records Management Policy • Business Continuity Management Policy • Third Party Risk Management Procedures • Contracting Standards and Procedures • Exception Policy and Procedures • Code of Business Conduct and Ethics

Global Third Party Risk Management Policy

Version No. – Effective Date	V0.1 - October 2017
Policy Owner	Vice President of Third Party Risk Management
Required Approving Body	Office of Enterprise Risk Management

Revision History

Version	Release Date	Summary of Changes	Policy Owner
1.0	October 2017	Initial Policy	Betsy Alaniz

Glossary

Term	Definition
Associates	An operating entity that is not owned by Crawford but provides services under the Crawford brand
Business Relationship Owner (BRO)	Have primary responsibility for managing third party relationships and represent the first line of defense for ensuring compliance with the TPRM Policy; may be a business line or product line manager
Company	Means Crawford & Co
Compliance Risk	Refers to the failure or deficiencies in complying with legal or regulatory requirements which may subject Crawford to fines or other disciplinary remedies.
Consequence	Outcome or impact of an event and may be expressed qualitatively or quantitatively. There can be more than one consequence from one event. Consequence can be positive or negative. Consequences are considered in relation to the achievement of objectives.
Control	Measure to modify risk. Term often used interchangeably with risk 'treatment'. Specifically, controls are the result of risk treatment. Controls include any policy, process, device, practice or other actions designed to modify risk. See Risk Treatment.
Event	The occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences.
Exposure	Extent to which the Company is subject to an event.
Foreign State & Country Risk	Refers to the risk arising from possible changes in the business environment that may adversely affect operating profits or the value of assets in the country. For example, financial factors such as currency controls, devaluation or regulatory changes, or stability factors such as civil unrest, war and other potential events which may contribute to Crawford's operational risks.
Financial Condition Risk	Refers to third party's financial condition and the ability of the third party to deliver service and product obligations which may impact the delivery of services to Crawford or Crawford

	clients.
Inherent Risk	The intrinsic risk prior to considering any controls in place.
Insurance Risk	Assurance that insurance limits and liabilities are commensurate with the level of sensitivity and/or criticality of services provided to Crawford or Crawford's clients.
Likelihood	General description of probability or frequency. It can be expressed qualitatively or quantitatively.
Management, Senior	Means the Executive Management of the Company.
Operational Risk	Refers to disruptions, delays, or other events causing a denigration of transaction processing, customer service, IT & physical security and data privacy, internal controls, capacity availability such as business continuity management and disaster recovery, etc. which may impact the availability, confidentiality or integrity of Crawford's services and products.
Personnel Health & Safety	Refers to the due diligence required to ensure a third party meets regulatory health and safety requirements.
Procurement	Responsibility for ensuring understanding the terms and conditions of trade and to ensure competitive advantage within the supply chain
Regulatory Bodies or Authority	Federal, state or local agency that has a legal and/or regulatory power over an aspect of the Company's activities including the capacity to initiate prosecutions, punitive actions or sanctions.
Risk	Risk is the exposure to unexpected financial or other damage arising from Crawford's business activities.
Risk Acceptance	Informed decision to take a particular risk. Risk acceptance can occur without risk treatment or during the process of risk treatment. Risks accepted are subject to monitoring and review.
Risk Analysis	The systematic process applied to understand the effect of the uncertainty of the risk on the Company's goals and objectives.
Risk Appetite	The Company's approach to assess and eventually pursue, retain, take or turn away from risk. The amount of risk an organization is willing to accept

	in pursuit of value. It reflects the entity's risk management philosophy and influences the entity's culture and operating style.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Tolerance	The acceptable level of variation relative to achievement of a specific objective. Tactical and operational; operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives
Residual Risk	The level of risk that remains after assessing the effectiveness of the controls, management strategies and other mechanisms currently in place to mitigate a particular risk.
Risk Identification	The process of determining what might happen, how, when and why.
Risk Management	Risk management is the culture, processes and structures that are directed towards realizing potential opportunities while managing adverse effects.
Stakeholders	Those people and organizations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk.
Strategic Risk	Refers to inadequate management planning and oversight of third party suppliers leading to a lack of understanding, mitigation, and control of risks by Crawford for the services or products provided by the third party.
Reputational Risk	Refers to errors, delays, or omissions in outsourced services and products which may become public knowledge and / or directly affect customers that may impact Crawford's brand.
Risk Treatment	The process of selection and implementation of measures to modify risk
Secondary Supplier Transparency (4th Party Risks)	Refers to oversight of subcontracted services for the third party. (i.e. "suppliers to suppliers") and the level of risk management that is applied to these secondary suppliers.
Supply Chain Management	Overall responsibility for managing interdependencies between the line of business and the required vendors and suppliers to deliver a quality service conforming to the terms of the

	contractual agreement
Support Risk	Refers to the failure or inability of the third party to perform within contracted Service Levels for the services or products provided by the third party to Crawford.
Third Party	A third-party relationship is any business arrangement between Crawford & Co. and another entity, by contract or otherwise
Vendor Manager	Responsible for review of the management of the vendor's services, SLA / KPI / KRI Performance metrics, modification of SOWs to accurately reflect the scope of services being provided; this role sits within the Third Party Oversight function