4Thought Marketing Third-Party Risk Management Policy

Table of Contents

Security Policy Home

Last Update:

October 27, 2025

Overview and Background

4Thought Marketing (hereinafter referred to as 4Thought) uses Third Parties to provide products or services in support of our business operations. Such outsourced relationships may benefit 4Thought by reducing costs, improving performance, staff augmentation, increasing business competitiveness, accessing specific expertise, and establishing distribution channels. However, the ETeam and the Partners recognize that 4Thought's reliance on third-party relationships presents risks that must be identified, assessed, and managed. Failure to manage these risks can expose 4Thought to financial loss, litigation, or other damages, or may even impair 4Thought's ability to service existing customer relationships or establish new ones.

Statement of Purpose

This policy aims to establish standards and guidance relating to 4Thought's management of its third-party relationships and the associated inherent and residual risks presented by those third-party relationships. These risks are present when 4Thought engages with third parties to provide products and services directly to 4Thought for the benefit of its internal operations, employees, investors, or customers. Furthermore, this document provides the structure for identifying, assessing, controlling, monitoring, and reporting on risks related to 4Thought's use of third parties per applicable laws, safe and sound business practices, and, as applicable, NIST guidelines (NIST SP 800-53, SP 800-161).

Policy Statement

Relationships with third parties are fundamental to 4Thought's ability to maintain its operations and offer products and services to its employees, customers, and investors. However, 4Thought's use of third parties does not diminish its responsibility to ensure that the activity is performed safely and soundly and complies with applicable laws. Therefore, we have established the Third-Party Risk Management Policy (hereinafter referred to as the policy) to formally define the framework, tools, roles, responsibilities, scope, and components needed for a fully functioning Third-Party Risk Management program. The framework shall comply with all applicable laws and regulatory guidelines. Accordingly, this policy sets forth the requirements for the effective identification, assessment, and management of these risks.

Terms

Third Party

The term third party broadly covers similar terms such as vendor, supplier, providers, and the like. The term third party relates to any person, independent consultant, or form of a legal entity, including but not limited to: vendors, service providers, suppliers, processors, business partners, marketers, or other third parties, with whom 4Thought contracts for purposes of obtaining products or services, or who collaborate with 4Thought in providing products and services in the marketplace.

Third-Party Risk Management and Oversight

Third-Party Risk Management is the formalized process of identifying, assessing, and mitigating risks presented to 4Thought, its employees, investors, and customers due to the improper supervision or mismanagement of the following: data, operations, compliance, and financial condition concerning those external parties with whom 4Thought has a relationship. The term Third-Party Risk Management, hereinafter referred to as TPRM, is also inclusive of all reporting, governance, and oversight activities necessary to ensure the safe and sound engagement with 4Thought's third parties.

Scope

TPRM applies to business arrangements between a third party and 4Thought by contract or otherwise, to obtain products or services.

All 4Thought employees, independent contractors, and consultants are subject to this Policy if they engage third parties for the Company's direct or indirect benefit.

Third Parties Not In Scope Under This Policy

The following third-party relationships have been excluded from this Policy:

1. Relationships with Customers
2. Relationships with Investors
3. Relationships with Employees
4. Relationships with public utility providers
5. Relationships with emergency services such as police or fire departments
6. Relationships with government agencies, taxing authorities, regulatory bodies, and courts

Pre-existing Third-Party Relationships

It is the responsibility of the 4Thought Security Team and ETeam to ensure compliance with this Policy regarding third-party relationships maintained by 4Thought. It is possible that certain existing third-party relationships (and contracts) do not comply with all policy aspects. However, 4Thought is obligated to renegotiate, to the extent possible, any contract terms and conditions of existing third-party contracts to comply with this policy and the related processes. Renegotiation shall occur at the first potential and reasonable opportunity (i.e., contract negotiation).

Third-Party Risk Management Oversight

The Security Team and the ETeam are ultimately accountable for the TRPM policy, program, and processes' oversight and effectiveness, and must ensure that the TPRM program operates according to applicable federal and state laws, rules, regulations, internal policies, and procedures. They achieve this through the following:

Policy Management and Approval

The CEO and Security Team of 4Thought initially approved and oversaw the Third-Party Risk Management and Oversight Policy and annually review and, if necessary, update the Policy.

Approval of Critical Third Parties

The 4Thought Security Team and ETeam, or their designated committee, are responsible for the decision to approve the addition or termination of third-party relationships considered critical to 4Thought. Such approvals are mandatory in advance of final contract execution with any material third party.

Periodic Review of Critical Third Parties

The 4Thought Security Team and ETeam, or their designated committee, shall periodically review third parties considered critical to 4Thought's operations. They must consider the related risk assessments, monitoring, compliance, business continuity, financial health, and overall performance of those material third parties.

Staffing and Resources

Senior Management shall allocate sufficient qualified staff (internal or augmented) to provide the necessary oversight and monitoring of significant third-party relationships. Sufficient resource capacity is maintained to execute essential TPRM processes effectively, especially those requiring specialized expertise. And to ensure all critical and high-risk rated third-party relationships are assessed, monitored, and managed commensurate with the product or service's risk.

Geographic Restrictions and Sanctions Compliance

Purpose

To ensure that 4Thought engages only with third parties operating in jurisdictions that comply with applicable trade, sanctions, and data-protection regulations, and to prevent exposure to undue geopolitical or legal risk.

Prohibited Jurisdictions

1. 4Thought **does not engage, directly or indirectly**, with any third party (including

subcontractors, affiliates, or agents) that is:

1. Domiciled in, or conducting material operations from, a country or territory subject to comprehensive sanctions or embargoes imposed by the:
    - United States Department of the Treasury's Office of Foreign Assets Control (OFAC);
    - United Nations Security Council;
    - European Union; or
    - United Kingdom Office of Financial Sanctions Implementation (OFSI).
2. Located in or controlled from any region currently under international sanction, including but not limited to **Iran, North Korea, Syria, Cuba, Crimea, Donetsk, and Luhansk**.

High-Risk Jurisdictions

1. For countries identified by credible international authorities (e.g., FATF, Transparency International, U.S. State Department) as high risk for corruption, data protection deficiencies, or human rights violations, 4Thought shall:
    1. Conduct **enhanced due diligence** before onboarding or renewal.

2. Obtain documented approval from **Legal and Information Security**.

3. Require the vendor to implement compensating controls and contractual safeguards appropriate to the level of risk.

Data Protection Adequacy

1. Where a third-party processes data subject to privacy regulations (e.g., GDPR, CPRA) and operates in a jurisdiction **lacking adequacy status**, 4Thought will require:
    1. Valid **Standard Contractual Clauses (SCCs)** or **Binding Corporate Rules (BCRs)**; and

    2. Clear documentation of data transfer mechanisms and hosting locations.

Ongoing Monitoring and Escalation

1. The **Third-Party Risk Management (TPRM)** function shall:
    1. Continuously monitor sanctions lists and country risk ratings;

2. Re-evaluate existing vendor relationships if geopolitical conditions materially change; and

3. Escalate any potential violations to the **Compliance Officer** for immediate review and remediation.

Exceptions

1. Any exception to the above restrictions requires:
    1. Written justification approved by **Legal**, **Compliance**, and **Executive Management**; and

    2. Documentation within the vendor's risk file outlining compensating controls, rationale, and approval date.

Data Residency Requirements

Approved Data Storage Locations

4Thought data may only be stored or processed in the following approved jurisdictions:

- United States (US)
- Canada (CA)
- European Union (EU) member states

Third-Party Data Handling

All third parties that store, process, or have access to 4Thought data must:

1. Clearly document all data storage and processing locations in their contracts
2. Provide written confirmation that data will remain only in approved jurisdictions
3. Implement appropriate technical and organizational measures to prevent data transfer to non-approved locations
4. Notify 4Thought immediately if data location requirements cannot be maintained

Data Residency Verification

During due diligence and ongoing monitoring, the TPRM team shall:

1. Verify the physical location of all data centers and processing facilities
2. Confirm compliance with data residency requirements
3. Document any data transfers or replication between approved jurisdictions
4. Ensure appropriate data protection agreements are in place for any cross-border data transfers within approved jurisdictions

Exceptions

Any exception to data residency requirements must be:

1. Approved in writing by the Security Officer and Legal Counsel
2. Supported by appropriate risk mitigation measures
3. Documented in the vendor risk file with clear justification

Organizational Structure and Responsibilities

The Security Team and ETeam

The Security Team and ETeam are accountable for ensuring the effectiveness, safety, and soundness of TPRM, executed through the following activities:

- Confirming that risks related to third-party relationships are managed in a manner consistent with 4Thought's strategic goals and risk appetite
- Approving the policies that govern third-party risk management
- Approving, or delegating to, an appropriate committee reporting to the Board, approval of contracts with third parties that involve critical activities
- Reviewing the results of Management's ongoing monitoring of third-party relationships involving critical activities
- Confirming that Management takes appropriate actions to remedy significant deterioration in performance or address changing risks or material issues identified through ongoing monitoring
- Reviewing the results of periodic independent reviews of the third-party risk management process

Senior Management

Senior Management is accountable for executing and implementing third-party relationship risk management strategies and policies across the organization. Management is also responsible for ensuring that organizational structures, management, and staffing (level and expertise) are in place to properly manage third-party risk and comply with all legal and regulatory requirements. Furthermore, Senior Management is accountable for the following:

1. Developing and implementing 4Thought's third-party risk management process
2. Confirming that 4Thought has an appropriate system of internal controls and regularly tests the controls to manage risks associated with third-party relationships
3. Confirming that 4Thought's compliance management system is appropriate to the nature, size, complexity, and scope of its third-party business arrangements
4. Confirming that appropriate due diligence and ongoing monitoring are conducted on third parties
5. Presenting results to the ETeam when making recommendations to use third parties that involve critical activities
6. Escalating significant issues to the ETeam
7. Reviewing and approving contracts with third parties
8. Confirming that third parties comply with 4Thought's policies and reporting requirements

9. Providing that third parties test and implement agreed-upon remediation when issues arise

10. Terminating business arrangements with third parties that do not meet expectations or no longer align with 4Thought's strategic goals, objectives, or risk appetite

11. Maintaining appropriate documentation throughout the third-party risk management lifecycle

Third-Party or Vendor Owners, aka Engagement Managers

Third-party or vendor owners are expected to support Senior Management and follow this policy by:

- Completing the Planning, Risk Assessment, Contracting, and Monitoring phases of TPRM
- Notifying TPRM Management of intended new or changing third-party relationships that may impact its operations
- Maintaining third-party information within the third-party management system of record
- Validating the accuracy and content of the services provided by their third parties
- Completing the periodic risk assessment process
- Issue identification and reporting during any phase of TPRM

Technical Marketing Automation Services (TMAS) Team

The TMAS team provides technical expertise and support for third-party relationships involving marketing automation technologies and related services. The team works closely with the Security Team and vendor owners to ensure appropriate technical controls and monitoring are in place.

Independent Reviewers

4Thought's internal Security Team or an independent third party may perform the reviews. Senior Management confirms that the results are reported to the ETeam. Reviews include assessing the adequacy of the organization's process for:

1. Confirming third-party relationships align with the 4Thought's business strategy
2. Identifying, measuring, monitoring, and controlling risks of third-party relationships
3. Understanding and monitoring concentration risks that may arise from relying on a single third party for multiple activities or from geographic concentrations of business
4. Responding to material breaches, service disruptions, or other material issues
5. Involving multiple disciplines across the organization as appropriate during each phase of the third-party risk management lifecycle
6. Confirming appropriate staffing and expertise to perform risk assessment, due diligence, contract negotiation, and ongoing monitoring and management of third parties

7. Confirming oversight and accountability for managing third-party relationships (for example, whether roles and responsibilities are clearly defined and assigned, and whether the individuals possess the requisite expertise, resources, and authority)

8. Confirming that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties

Legal Team or Legal Council

Legal support is provided via outside counsel as needed. As the Security Team or the CEO requires, qualified external legal counsel may review prospective third-party arrangements and contracts. Any legal counsel consulted.

Documentation and Reporting

4Thought properly documents and reports on its third-party risk management process and relationships to facilitate accountability, monitoring, and risk management associated with third parties. Regular reporting is provided to appropriate stakeholders and may include:

- Analysis of costs associated with each activity or third-party relationship, including any indirect costs

- A current inventory of all third-party relationships, identifying those relationships that involve critical activities

- Reports for critical relationships detailing the current status of risk assessments, due diligence results, contract status, performance, service levels, internal control testing, and other ongoing monitoring results

- Third-party service disruption, security breaches, or other events that pose a significant risk to 4Thought

- Third-party risk management program metrics, issues, tests, or other relevant information

Risk Management Overview

4Thought's Third-Party Risk Management process is comprised of five elements, including:

- Planning and Risk Assessment

- Risk-Based Due Diligence and Third-Party Selection

- Contract Structuring, Negotiation, Execution, Maintenance

- Ongoing Oversight and Monitoring

- Termination

These elements apply to all third-party activities; however, the extent and scope required for any third party are dependent on numerous factors. 4Thought's risk identification and management process contemplates the nature of the third-party relationship, the complexity, and magnitude of the activity provided, and the risks identified related to the third-party relationship. Risk identification, assessment, and monitoring are appropriately scaled and commensurate with the risk.

Planning

Before entering into a third-party relationship, 4Thought defines the nature of the proposed relationship to ensure that it aligns with the organization's strategic goals and objectives and to identify how it might align or impact strategic initiatives. The overall value of the proposed relationship is evaluated to determine if the benefits of such an arrangement outweigh the estimated cost. And, to ensure other relevant factors are considered and evaluated, such as the complexity of the arrangement, the technology needed, the likelihood of foreign third-party activities, and any potential impact on the organization's employees. To provide adequate oversight of third-party relationships, 4Thought must determine if sufficient resources are available. And, whether staffing levels and expertise need to be adapted for 4Thought to address the business arrangement effectively. Additionally, 4Thought defines a suitable contingency plan if the activity must be transferred to another third party or brought in-house.

Risk Assessment

Each prospective third-party relationship and subsequent engagement is assessed for the inherent risk posed to 4Thought based on the nature of the products or services provided, and determines whether the third party is critical or non-critical. The inherent risk assessment assesses distinct categories of risk and the total risk of the relationship.

- Specific risk areas examined may include:
    1. Business Continuity Risk

    2. Compliance Risk

3. Financial Risk
4. Legal Risk
5. Cyber Risk
6. Country Risk
7. Transactional Risk
8. Concentration Risk*
9. Information Security Risk
10. Privacy Risk
11. Strategic Risk
12. Operational Risk
13. Reputational Risk

*Note: As a small organization, 4Thought acknowledges that concentration risk may be inherent in certain vendor relationships. While formal concentration risk thresholds are not currently established, the TPRM team will monitor for over-reliance on single vendors for critical services and escalate concerns as they arise.

Unless otherwise authorized by TPRM, all third-party engagements must have an Inherent Risk Rating. To assess risk accurately, 4Thought's employees must utilize the tools, formats, and systems defined by TPRM.

Criticality

As each third-party engagement is risk-rated, a small subset of third-party engagements is identified as critical. The distinct and separate classification of critical serves to identify the most essential and highest-risk business activities provided by third parties to 4Thought in service of its operations, employees, investors, and customers. Third parties deemed "Critical" or "High Risk" are subject to additional monitoring or other internal controls as determined by 4Thought management.

Critical

A third party is considered critical when performing an activity deemed crucial to the organization's operations or is the sole provider of an essential business function. Additionally, any sudden interruption of that activity (or failure to perform it as required) can cause significant disruption to 4Thought's core operations if not quickly and easily remedied.

A third party is considered critical when:

1. The sudden loss/disruption of this third party would cause significant disruption or regulatory scrutiny to the business and its critical functions.

2. The sudden loss would impact 4Thought customers.

3. Service disruption would be a negative impact on 4Thought's operations if the time to restore were more than 24 hours.

Non-Critical

The third party does not perform a mission-critical business function or serve as the sole provider of an essential function. The sudden loss of the third party's product or services would not cause significant disruption to operations.

Risk Ratings

Standard TPRM risk ratings are as follows: High (H), Moderate (M), and Low (L) ratings are the baseline rating assigned to third-party engagements. As applicable, these ratings are utilized as both inherent and residual risk ratings.

Low

- The relationship's nature and the third party's risk profile present little to no risk, and minimal ongoing monitoring is warranted.

- The third party has minimal/no access to or interaction with customers or confidential employee, investor, or customer information.

Moderate

- The nature of the relationship or the third party's risk profile presents some level of risk, and periodic oversight is necessary.
- The third party has limited access to or interaction with customers or confidential customer information.

High

- The nature of the relationship and the third party's risk profile present a significant risk that must be mitigated and requires frequent oversight through due diligence and monitoring activity.
- Notwithstanding any other risk factors presented, any third party with regular access or interaction with customers and confidential customer information is deemed "high risk."

Residual Risk

Inherent risk represents the amount of risk existing in the activity in the absence of controls. The inherent risk assessment identifies the types of risk associated with the product or service and its significance to 4Thought. Once further evaluations and due diligence are complete, the validation of sufficient controls, practices, and assurances helps determine the residual risk of the engagement.

A residual risk rating is used solely to determine if the remaining risk is within the 4Thought's risk appetite, and if additional risk mitigation actions are warranted before entering into a business relationship with a third party.

Residual risk ratings are never used in place of inherent risk ratings when determining TPRM risk management activities throughout the TPRM lifecycle.

Risk Assessment Implementation

The risk assessment methodology outlined in Sections 13.1 through 13.3 shall be implemented using standardized assessment tools that ensure consistent and objective evaluation across all third-party relationships.

The assessment process involves:

1. **Initial Risk Profiling**: Evaluating the third party against the thirteen (13) risk categories identified in Section 13

2. **Criticality Determination**: Applying the criteria in Section 13.1 to classify the engagement as Critical or Non-Critical

3. **Risk Rating Assignment**: Using the definitions in Section 13.2 to assign an inherent risk rating (High, Moderate, or Low)

4. **Residual Risk Calculation**: Following due diligence completion, reassess the risk level based on validated controls and mitigations

This methodology may be implemented through:

- Standardized risk assessment questionnaires and scorecards
- The TPRM Management System of record (reference Section 19)
- Automated risk scoring platforms, as available
- Consistent documentation templates are maintained by the Security Team

All third-party risk assessments must use this standardized methodology to ensure objectivity, repeatability, and appropriate risk-based oversight throughout the vendor lifecycle.

Due Diligence

Overview

Comprehensive, risk-based due diligence processes are appropriately scaled to ensure that contracted engagements meet strategic and financial objectives, data security and privacy standards, and support operational and contractual requirements.

Completion of Due Diligence Before Contract Execution

Due diligence is completed and formally documented before 4Thought and a third party enters a contract. Due diligence is then performed periodically during the relationship.

Before renewing critical or high-risk contracts, satisfactory due diligence must have been completed within a calendar year. For third parties rated Moderate or Low risk, due diligence requirements and intervals are determined by TPRM, based on the engagement's significance, complexity, and impact.

Scope

Critical and high-risk third parties are subject to rigorous due diligence to assess their control environment's sufficiency, resiliency, financial condition, reputation, compliance with all applicable laws and regulations, and the ability to service 4Thought's operations. This process requires the third party's provision of internal documents such as policies, procedures, complaint logs, financials, business continuity, disaster recovery plans, and testing results, and independent third-party certifications to evidence the sufficiency of their control environment.

The scope of due diligence documentation requested is risk-based and calibrated to both the nature of the relationship and the evidence necessary to assess controls accurately. Additionally, other required evidence may substantiate controls, including on-site visits (when conditions allow) and interviews with key personnel.

Outsourced Due Diligence Collection and SME Review

Under certain circumstances, 4Thought may outsource the due diligence process or a specific component thereof. The decision to outsource due diligence document collection or SME review may be warranted based on work volume, the technical nature of the area evaluated, the third party's geographic location, or the need for greater objectivity or independence in the review. However, it is 4Thought's responsibility to determine whether the external ratings regarding the strengths and weaknesses of controls are sufficient and how those ratings are applied when calculating residual risk.

Periodic Risk Assessments and Ongoing Monitoring

Overview

4Thought maintains sufficient oversight of third-party activities and adequate quality control over those products and services provided through third-party arrangements to minimize exposure to potential material financial loss, reputation damage, and supervisory action. Management must review the third party's operations to verify that they are consistent with the written agreement terms and managed risks. 4Thought must confirm the third party's compliance with applicable federal and state laws, rules, regulations, and internal policies.

A third party's risk profile may change over time, and overall risk can increase or decrease due to numerous factors. Per best business practices and regulatory guidance, 4Thought continuously monitors third parties' risk, performance, and relationships' strategic value. Risk-based requirements determine the prescribed intervals and standards for these periodic reviews and monitoring.

Periodic Risk Assessments

Validation of the third-party risk profile dictates periodic risk review and assessment. These evaluations require third parties to provide updated or current due diligence documentation and possibly additional documentation as necessary.

Risk assessment intervals shall be as follows:

- **Critical and High-Risk Third Parties**: Annual assessment required (within 12 months of previous assessment)

- **Moderate Risk Third Parties**: Assessment required every 18 months
- **Low Risk Third Parties**: Assessment required every 24 months
- **In no event shall any third-party assessment interval exceed 2 years**

These assessments will be performed by the TPRM team or the Security Team. The team shall consider risks specific to the third party's industry, service, product category, or other relevant matters that contribute to the assessment when necessary.

Additional Risk Assessment as Necessary

Additional periodic assessments are considered under the following circumstances:

1. Material changes in a third party's business practices, financial position, reputation, or similar.
2. Increased reliance on the third party and its services.
3. Changes in applicable law or regulation impact the third party's product or service.
4. Increased media attention, negative publicity, or industry scrutiny related to the third party.
5. Regulatory enforcement actions or industry-related guidance impacting the third-party

relationship.

6. Increased or emerging risk within the third party's industry, service, or product category.

Contractual Standards

Overview

Third-party relationships shall be documented by written agreements that appropriately and adequately consider the contemplated relationship and provide 4Thought with appropriate protections and controls, consistent with prudent business practices. This policy collectively refers to all legal agreements as "contracts." The term contract refers to all written legal agreements facilitating the use of products or services to 4Thought, including statements of work, purchase orders, licensing, servicing, marketing agreements, and other similar written agreements.

Contract Terms and Provisions

Contracts should include clear and concise language regarding the arrangement between 4Thought and the third party. Contracts originating from 4Thought are preferred. However, custom agreements prepared by legal counsel or proposed agreements offered by the third party are acceptable when key terms and provisions are reasonably represented. If possible, the contract should protect 4Thought by providing full audit rights. Other contract terms and conditions may vary based on the relationship's risk and the complexity and significance of the products and services.

Analysis of Contract

4Thought shall undertake analysis and review of any proposed agreement and ensure that the proposed terms are consistent with 4Thought standards and effectively manage the third-party risks identified during the risk assessment and the due diligence process. Contracts for critical or high-risk products and services must sufficiently address the following:

1. Cost and compensation
2. Performance standards
3. Reporting
4. Audit
5. Confidentiality and security
6. Customer complaints
7. Business resumption and contingency plans
8. Default and termination
9. Dispute resolution
10. Ownership and license

11. Compliance

12. Limits of liability

13. Use of subcontractors

14. Indemnification

15. Data residency and protection requirements

16. Geographic restrictions

Contract Execution

4Thought policy dictates that third-party contracts are not executed until due diligence has been completed and any issues requiring pre-contract remediation are satisfied. The Subject Matter Expert who identifies the original issue must review the evidence of closure and document whether the issue has been resolved adequately.

Additionally, key terms and provisions missing from the initial contract are negotiated to ensure inclusion in renewed contracts or other documented agreements.

Contract Management

Contract management is achieved by monitoring third-party risk, performance, and the closure of open issues.

Contract renewal dates and termination dates shall be actively managed and monitored to ensure 4Thought knows its contractual rights and obligations in managing its third-party relationships. Further attention shall be given to important dates and agreed-upon items in the contract between 4Thought and the third party.

Contract Termination

If 4Thought determines that a third-party relationship must be terminated, an evaluation is conducted to determine the impact this will have on any business relationships or customers affected by that decision. Procedures and internal controls to reduce the possible negative impacts of termination are identified. Action plans must be developed to address other operational events related to termination.

Contract Non-Compliance

4Thought places particular emphasis on its ability to terminate agreements with third parties who fail to adhere to contract requirements or otherwise place 4Thought in an unacceptable risk position at any time during the term of the agreement.

Ongoing Monitoring

Monitoring intervals and requirements, defined by TPRM, are risk-based and appropriate for the specific third-party relationship.

Monitoring activities

4Thought monitors the third party's operations to verify that they are consistent with the written agreement terms and may include:

1. Reviewing reports relating to the third party's performance in contractual requirements and performance standards, including both service level agreements and quality standards, with appropriate follow-up as needed.

2. Evaluation of the third-party relationship's overall effectiveness and the relationship's consistency with 4Thought's strategic goals.

3. Confirmation that the third party is meeting its financial obligations to others.

4. Reviewing audit reports or other third-party reports and follow up on any needed corrective actions.

5. Monitoring for compliance with applicable laws, rules, and regulations.

6. Assessing the effect of changes in key third-party personnel involved in the relationship with 4Thought.

7. Administering testing programs for third parties with direct interaction with customers.

8. Reviewing customer complaints about the products and services provided by the third party and the subsequent complaint resolution.

9. Meeting with third-party representatives to discuss performance and operational issues.

10. Verifying compliance with geographic restrictions and data residency requirements.

Enhanced Oversight

Enhanced oversight rules apply to any third-party relationship deemed critical or high-risk. As appropriate, these reviews' status and findings are reported to the necessary stakeholders, including the 4Thought Security Team and ETeam. At a minimum, critical and inherently high-risk third parties undergo a periodic risk assessment within one calendar year of completing initial due diligence or previous assessment.

Escalation and Corrective Action

Third-party relationships or third-party products or business practices pose an extreme risk subject to enhanced oversight processes/or corrective action. When necessary, they are escalated to the CEO or Partners for review. Factors warranting escalation may include, but are not limited to:

• Heightened third-party risks or other business concerns identified during initial due diligence, periodic assessments, ongoing monitoring, or by other means
• The third party cannot, or will not, provide sufficient documentation to satisfy due diligence requirements or perform its duties and responsibilities
• Proposed third-party relationships or third-party practices appear to be under scrutiny or criticism by state or federal regulators, or the subject of heightened litigation or increasing reputational risk
• Failed business continuity or resumption within stated recovery time objectives.
• Declining financial health, bankruptcy, or other material condition, impacting the third party's ability to provide products and services to 4Thought
• Heightened or emerging risk within the third party's industry, product, or service category
• Violations of geographic restrictions or data residency requirements

Corrective Action Documentation

Issues or deficiencies raised with senior management and/or other appropriate stakeholders must be addressed promptly, mitigated, and escalated as required. Escalations and corrections are documented and tracked appropriately.

Third-Party Non-Compliance

If any third party fails to cooperate with the corrective action process or otherwise fails to address deficiencies promptly, the matter is referred to the Security Team for evaluation and action. 4Thought evaluates all legal and contractual rights and remedies to avoid or mitigate continued exposure to third-party risks.

Termination

The organization may terminate a third-party relationship for various reasons, such as expiration of or dissatisfaction with the contract, a desire to seek an alternate third party, a desire to bring the activity in-house or discontinue the activity, or a breach of contract. 4Thought acknowledges the possible risks associated with the termination of a third-party contract or relationship. The 4Thought approaches each third-party termination in a manner appropriate to the relationship and considers the type of termination being undertaken.

For critical activities, there must be a documented plan to transition services in a timely manner to another third-party provider or bring the service in-house. If there are no alternate third-party providers, activities are transitioned to another third party, brought in-house, or discontinued.

In the event of contract default or termination, the following factors and others are considered:

1. Capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise

2. Potential third-party service providers to which the services could be transitioned

3. Risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship

4. Handling of joint intellectual property developed during the course of the business arrangement

5. Risks to 4Thought if the termination must happen due to the third party's inability to meet expectations

Systems of Record

The system of record (TPRM Management Spreadsheet) preserves third-party agreements for ongoing tracking and follow-up monitoring based on risk and criticality. The TPRM Spreadsheet notes special contract terms (renewal or expiration dates, notice requirements, and others). A software tool for tracking third-party risk management activity and managing third-party documentation provides multiple control and notification layers to assist in and ensure the proper control over document collection, storage, and timelines.