

White Paper

Third Party Risk Management

Reducing Risk from a Third Party: *A Practical Operational Approach*

Introduction

When an organization outsources internal functions such as human resources, or information technology, or when even just when an external entity has access to or control of customer, sensitive, or even proprietary information the risks to information confidentiality, integrity and availability increase significantly. At the same time there are often valid business reasons for accepting such risk. However, the business equation should take into account the cost of due diligence and due care (explained below). Successful outsourcing depends on good due diligence during Third Party selection and ongoing due care during the relationship. This paper addresses the information risk aspects of due diligence and due care as well as ingredients to accomplish to both

The aim of information risk management (IRM) is to identify and mitigate risks to information assets to an acceptable level to the business. Third Party Risk Management (TPRM) program is a subset of an organization's overall IRM program. The goal of a TPRM program is to identify and manage risks to the enterprise from its portfolio of vendors, service providers, and external business partners each of which aligns to the fundamental definition of those that “have access to or control of customer, sensitive, or even proprietary information”.

There is no secret to a successful Third Party Risk Management Program. There is no silver bullet or unique tool that solves this problem for an enterprise. Instead it is a matter of systematically building a program that meets your company's specific business and regulatory needs. Such a program needs to be built and managed at both the macro level of the enterprise as well as the micro level of managing the risk from each individual relationship.

This paper outlines an effective approach for Third Party Risk Management.

The Aeritae Approach

Aeritae suggests a common sense and organized approach to achieve effectiveness and efficiencies. To actually achieve such results means several important factors need to be considered. From management support, education and awareness campaign, internal and external processes defined, metrics, and effective communication are some of the foundational ingredients for a successful program. This governance should be outlined in the enterprise information security policies and further defined in a TPRM information security standard supported by appropriate operating procedures.

Lastly, an effective TPRM program needs to address both due diligence and due care. Due diligence involves appropriately assessing risk at the beginning of a relationship while due care is ongoing risk management.

Phase 1: Program Build Phase

To assure a defensible, risk-based due diligence approach, Aeritae recommends a Third Party Risk Management model based on the ISO 27001/27002 standard. This model gives the organization the ability to coordinate Third Party security with existing Information Security Management Systems (ISMS) and with other governance models such as COBIT and ITIL. A model should be process-based and risk-driven. It should provide metrics for management review and awareness as well as identifying opportunities for process improvement. It should also consider blending TPRM into the enterprise risk management methodology. During the build phase the following should be addressed:

- ▶ Top management must empower and support the program's need and value to the business as well as to meet regulatory requirements
- ▶ Given the organization's risk posture, security posture, and business requirements, a plan-the-plan approach to optimize Third Party Risk Management activities should be developed and approved. This includes:
 - Mapping out existing processes for Third Party due diligence and due care
 - Defining out existing TPRM roles and responsibilities
 - Relating TPRM to overall Third Party due diligence activities
 - Aligning TPRM to enterprise risk management goals
 - Defining and documenting the current state of the TPRM program.
 - Conducting a gap analysis between the approved security practices within the assessing entity to that of the Third Party to determine if they meet the assessing organization's information security policies or accepted standards, such as ISO

27002 or applicable regulations. The findings are then used to develop a plan for process improvement for the Third Party.

Implementation

Some guidelines for successful implementation include:

- ▶ Communicate roles and responsibilities within the TPRM to appropriate departments and individuals
- ▶ Provide training and instructions to related roles and business units
- ▶ Transition Third Party relationships into new program
 - *NEW CONTRACTS*
 - Establish the process to utilize the Third Party security assessment tools into everyday use
 - *EXISTING CONTRACTS*
 - Organize existing contracts into three primary dollar categories and evaluate each to identify if the Third Party has access to or control of customer, sensitive, or proprietary information
- ▶ Apply assessment tools to new and existing Third Party relationships where justified by risk or business requirements
 - Develop an approved internal questionnaire that will be delivered to the Third Parties to complete
 - Review the questionnaire containing the Third Parties answers and evidence list (if applicable). This can be accomplished with the internal business segment.
 - Complete any remote interviews, onsite assessment, or penetration testing and vulnerability scanning, as appropriate. (NOTE: The validation effort of the Third Parties information security posture should be commensurate with the data being controlled and the risk.)
 - Provide and communicate a plan for corrective actions for reducing identified risks. This communiqué report should be provided to the Third Party as well as the internal business line who owns the contract relationship for this Third Party. This communiqué will help the internal business line make effective business decisions to move forward with the Third Party (accepting the risk(s)) or not.
- ▶ Track risks or monitor Third Party remediate efforts to validate corrective actions are being addressed.
- ▶ Provide Third Party security assessments to business decision makers. Doing so helps to transition Third Party selection into risk-based decision process for the business line segment.
- ▶ Create and report monthly, quarterly, and yearly statistics

- ▶ Establish and conduct annual reviews of at least the “high” risk rated vendor and update their risk status.
- ▶ Create or revise Third Party security assessment tools as needed

Due Diligence

Information risk assessment and management is only one aspect of the due diligence effort. Vendor viability, service or product quality, delivery, and financial issues all play an aspect but are primarily the job of the vendor management group.

The role of Information Security is to identify risks, recommend and implement mitigating measures and report the results to the business owner who owns the contract relationship between the internal business segment and the Third Party. Information Security should work with the legal department to ensure that the Third Party agreement meets the information security requirements that should be defined in the TPRM information security standard.

A typical Third Party agreement should contain elements of risk based on:

- ▶ Information technology issues, such as extranets and remote access
- ▶ Security issues, such as the exchange and processing of confidential information
- ▶ Third Party issues, such as supplier viability and contractual performance

A risk assessment is a critical aspect of risk identification and provides the bases for risk mitigation and ongoing due diligence. The level of effort and detail should be commensurate with classification of the data that the Third Party has access to or control of. All Third Parties should be classified based on the sensitive data that is accessed, stored or processed as part of the business’s relationship.

Due Care: Ongoing Third Party Risk Management

The due care phase of Third Party Risk Management implies that the Third Party will be subject to review and evaluation of its performance over time. This due care must be exercised for all risk aspects of the relationship, whether business, security or information technology, on a regular basis. The Aeritae Third Party Risk Management model provides our clients the tools needed to demonstrate that such due care is in place. Such items include:

- ▶ Establish and track a scheduled review cycle minimally for high risk rated Third Parties. If capable, for all Third Party security relationships
- ▶ The development of the long term re-evaluation/re-assessment activities
- ▶ Develop tools and forms for annual review (may be the same as the initial review)
- ▶ Incorporate guidance from Third Party Risk Management into the business processes for contract renewal or revision

- ▶ Manage Third Party Risk Management inputs and outputs
- ▶ Use risk management metrics to improve both Third Party relationships and the Third Party Risk Management program
- ▶ Such steps above demonstrate legal and regulatory compliance within Third Party relationships

Summary

In many business environments outsourcing is a key success strategy, allowing organizations to focus on their core competencies. However, the use of Third Parties to provide business solutions brings the added burdens of due diligence in Third Party selection and due care in Third Party oversight. The increasing pressure from legal and regulatory requirements will invariably add to the efforts of due diligence and due care. At the end of the day, the onus of responsibility falls squarely on the entity allowing a Third Party to have access to or control of customer, sensitive, or proprietary information.

The Aeritae Third Party Risk Management model is specifically designed to ease these burdens and meet the onus of responsibility. The model provides continuous assurance of both due diligence and due care to serve as evidence of doing the “right thing” as well as meeting regulatory requirements. Based on an internationally recognized and accepted standard, using assessments driven by risk management principles and processes designed to provide insight and metrics, Aeritae can assist organizations move to proactive, optimal Third Party Risk Management. Integrating Third Party Risk Management processes into an overall Third Party Risk Management program, and into enterprise risk management, our model provides the tools necessary to achieve defensible assurance and to meet regulatory requirements for both clients and regulators.

Aeritae Third Party Risk Management Offerings

Aeritae experience and expertise in this areas allows us to assist our clients with the both the enterprise level program design and build as well as implementation of due diligence, and development of the processes and tools to perform due care. Aeritae's offerings include:

Third Party Risk Management Program Development – Enhancement/building a client's Third Party risk management program

Third Party Portfolio Risk Manager - A set of outsourced services that includes prioritization, scheduling, and performance of high-level risk assessment and metrics reporting. Based on client's need/direction we also perform on-site assessments using ISO 27001, PCI-DSS, HIPAA, or BITS/SIG/AUP, Pen testing & vulnerability scanning, and provide Mitigation tracking & reporting.

Aeritae Information Risk Offerings...