THIRD-PARTY RISK

Solution Primer

Rafal Los
Director, Solutions Research
Office of the CISO, Optiv

James Christiansen
VP, Information Risk Management
Office of the CISO, Optiv

Introduction

In 1624, John Donne penned the famous words "No man is an island" as the opening verse to his Meditation 17. Today, with the digital age firmly upon us, these words ring true for individuals as well as enterprises. No enterprise is truly self-contained and able to operate autonomously. Herein lies perhaps one of the great challenges for enterprise security in our era.

As companies grow and become interdependent upon each other, the issue of third-party risk rises to the forefront in boardrooms across the globe. Whether the relationship is strategic and prominent, or operates in the background – the threats that each third party relationship poses to the enterprise is very real. Strategic outsourcing creates vast opportunities for efficiency and cost reduction while taking non-core functions of business and moving them to a third party. The unknown business risk taken on as a result of this type of relationship – whether it's a third-party market research firm, a credit card processor, or manufacturing partner – is a source of consternation for CISOs that must be managed more effectively.

The interdependency of connected systems and business relationships requires a strong third-party risk plan that extends beyond traditional IT. The initial step is often to take an IT-focused view and investigate third-party network interconnections and data handoffs; but ultimately this is simply just the first stage of work. Third-party risk must be analyzed across the various risk categories, including relationship and business profile risk perspective, to create a complete and actionable picture.

Meeting Business Needs

The focus on third-party risk is a necessary one, as companies' relationships with their suppliers, partners and various other third parties become more complex. The interconnected nature of computer systems, business processes and relationships requires that every enterprise be vigilant. Previously low-risk secondary relationships are now understood to potentially cause unexpected impact due to the increasingly complex, interconnected nature of business and technology. Every business process, exchange of data and touchpoint creates an opportunity for a mishandling of that data, or an avenue for a breach.

Third-party risk programs are designed to minimize surprises. Whether the company has ten third parties or ten thousand – having a defined program structure from which to identify, assess and provide fact-based guidance is crucial. This type of program approach relies heavily on fundamental capabilities like the identification of third parties across a very wide spectrum of relationships – which is no menial task. Any well-meaning employee with a corporate card and a desire to shortcut some slow-paced internal IT process can expose sensitive data if proper controls are not applied.

> Third-party risk programs are designed to minimize surprises. Whether the company has ten third parties or ten thousand – having a defined program structure from which to identify, assess and provide fact-based guidance is crucial.

For example, a business department like marketing or sales goes directly to a Software-as-a-Service (SaaS) provider to contract for services, effectively bypassing IT. This also circumvents normal due-diligence, regulatory compliance and the business controls that are designed to understand the type of data and exposure risk with the service.

While IT cannot identify, much less solve, all of the third party risk opportunities, identifying network interconnectivity and data exchanges is one way to get started. The first step is to look critically at the value of enterprise assets, such as intellectual property, and identify the business processes that use these assets. Then, mapping out critical business processes, while both potentially time consuming and difficult, leads to a much deeper understanding of how the company works and where hidden third party dangers may lie. Understanding how data flows in and out of the company may help identify some of those key relationships and opportunities for third-party risk identification. The key is to see this as more than just a security or even IT problem – it is a business problem.

The types of third-party relationships that can pose a risk are not simply direct exchanges of customer data. A third party managing the heating, ventilation and cooling (HVAC) system of the company's facilities often requires direct network access to manage the many digital controls and sensors remotely. This example of an Internet of Things (IoT) device increases complexity and adds further risk, as processes that were previously fully manual and analog are now becoming digital with network access.

From the business perspective, a third-party risk program works to significantly reduce unnecessary, and unknown, risk formed from third-party relationships. Having a strong third-party risk program aligned to business can aid in maintaining compliance with industry regulation, help with due diligence for obtaining cyber insurance, and support a holistic enterprise security strategy.

Third-Party Risk Defined

While **third-party risk** has been defined in many different ways, Optiv defines it as:

> *"The residual risk posed by external business relationships to the strategic, reputational, operational, transactional, financial, compliance or geopolitical aspects of an enterprise."*

Operationalizing Third-Party Risk

Program Drivers

It is important to understand the program drivers for a third-party risk program. Program drivers are the **business-relevant reasons a program approach is instituted** and help substantiate the business case for necessary funding, resources and leadership. Research shows there are three main drivers for this program approach:

- To identify, quantify and manage risk to the business attributable to external business relationships.
- To demonstrate compliance to various local, regional and country regulations and acceptable practices with respect to risk management.
- To minimize *unknown* exposure of enterprise sensitive, critical and proprietary assets through external business relationships.

Business Requirements

As program drivers help guide the development of the overall program, **business requirements** help define the initial deliverables. Operating a successful program means effectively meeting the requirements from the business stakeholders in a timely manner. Optiv Solutions Research and Development focused on developing a strong program built upon stakeholder input. The research team started this work by gathering a list of commonly identified business requirements for third-party risk programs across a representative sample of industry verticals, maturity and company size. As security executives build their third-party risk program, these are the business requirements that should be top-of-mind:

- Business alignment with clear relationship and risk ownership.
- Management of third-party relationships and accountability for compliance requirements of those relationships.
- Ability to quantify risk exposure cumulatively, and to line-of-business.
- Accountability for exceptions management and signoff.
- Define and understand risk using a set of criteria that includes strategic, financial, regulatory and delivery risk as mandated by regulatory and fiduciary responsibility for public sector directors.

Leveraging a Third-Party Risk Program

A third-party risk program addresses several strategic business and technology challenges. **First and foremost**, a mature third-party risk program enables the business to make smart technology decisions, highlighting where a vendor or third party may contribute to increased technology risk. Having information available to make an informed decision is critical in business, and these types of capabilities support strong vendor management and security practices. Through the identification and assessment of third parties and hard data on the risks those third parties pose to the enterprise, the security team becomes a tool of a more informed business.

Second, the program works to decrease the number of unknowns from a security perspective – minimizing network connections and data handoffs with third parties that have not been vetted and are an unknown threat. It has been proven repeatedly that even a small company with minor technology capabilities can pose a threat as a third party. *In fact, the smaller and less technically advanced the third party, the larger the risk they may pose.*

Minimizing unknowns is important, even if those unknowns are simply documented for the purpose of understanding current risks. For example, identifying and documenting a third party with access to sensitive data that has not been properly vetted raises awareness of the unknown risk, providing the opportunity to understand the risk level of the organization. Having known risks is a significant improvement over unknown, undefined risks. A third-party risk program that at minimum has a risk registry is an improvement over no information at all and provides a starting point for the enterprise.

Studying the evolution of operational third-party risk programs across various industry segments has provided an insightful perspective. Many third-party risk programs start out as technology endeavors – meaning that they start in enterprise security as a way to identify technical risks posed by network connectivity and data interchange from various technology partners. Over time as the program matures, it evolves to include other types of risk and moves from being security-centric to risk-centric in a model where security provides material support for the broader program. With outsourced enterprise IT growing over 50 percent, often contracted directly by the business leader, an ineffective third-party risk program may overlook some of the most significant areas of risk for the organization.

As complexity in business continues to increase at alarming rates with new partners, suppliers and strategic outsourcing, a third-party risk program is pivotal to meeting compliance goals and feeding security operations and strategy.

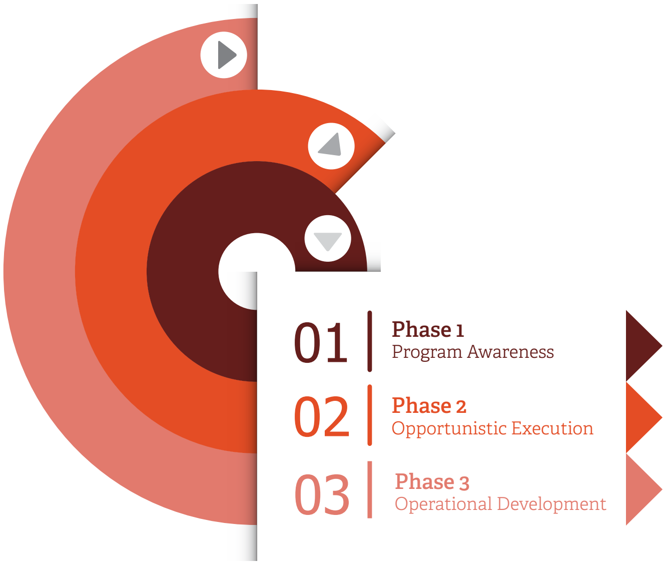
> Through the identification and assessment of third parties and hard data on the risks those third parties pose to the enterprise, the security team becomes a tool to a more informed business.

Developing a Program Strategy Approach

The foundation of any well-orchestrated security program is a strategy rooted in business alignment and supported by an appropriate balance of personnel, process and tools. Without a meaningful alignment to business objectives and available resources, the program will be unbalanced and produce irrelevant results. Inconsistent results are the antithesis of what CISOs want to achieve, thus the need to start by developing a strategy.

Research shows that enterprises large and small struggle with operationalizing their third-party risk programs – although the need is clearly present. Whether driven from a compliance mandate, or a board-level directive, third-party risk programs are quickly making their way to the top of the priority list. Anecdotal evidence shows that programs that are started without specific outcomes in mind and achievable milestones defined tend to fail to gain acceptance. Without that enterprise-wide acceptance, the program fails due to lack of budgetary dollars, leadership accountability and positive visibility.

Here we discuss a three-phased approach to planning, defining and beginning to operationalize a third-party risk program that is **outcome-based and capability-driven**. This is not meant to be a complete program framework, but outlines a high-level strategy that plots a course and provides research-backed guidance for the first few critical steps. Effectively we suggest goals, the resources necessary to achieve those goals, and provide high-level advice on achieving those goals. This three-phase approach is an aggregate of the in-depth five-step maturity model that is outlined more completely in the **Third-Party Risk Blueprint** (a separate publication).



In our model, key outcomes are broken out into three components: program **scope**, risk **assessment** and risk **treatment**. These key outcomes are meant to help the reader understand the purpose of the phase and give research-based confidence of common outcomes.

Phase 1 – Program Awareness

Key Outcomes

- **Program Scope** – Initially the goal of program development should be to start to quantify the program scope for a third-party risk program. Understanding scope helps bring clarity and understanding of long-term strategy and provides guideposts for the program across its lifecycle. The initial outcome should be to create a program scope that defines key stakeholders and their requirements and frames them into achievable activities. Having goals and rationale for those goals is paramount.

- **Risk Assessment** – At this initial phase, the goal is to define a basic, standards-based, repeatable assessment process. Odds are this will mean adopting something from an industry peer, utilizing an existing tool, or simply using experience to determine the highest risk areas of concern. Getting started is important, so adopting a general approach such as a generic questionnaire is a significant improvement over doing nothing.

- **Risk Treatment** – The way we treat risk initially is different than the way we will address it later on in program development. Treatment is limited in this early stage to a qualitative, often "gut feel" approach. This may go against intuition, but again since we are using a non-business-specific assessment approach there are issues that will simply "feel" inadequate. It's important not to dismiss this gut feeling. The way a third party responds to a questionnaire is just as important as the answers they give. Start by creating a risk register, documenting and reporting risk to business stakeholders in a qualitative way to build the foundation for the program going forward.

Components

- **People**
  - › A part-time person is likely the main resource at this stage of program development.
  - › Involvement of key business **stakeholders** (as champions) is crucial to gain acceptance across the broader business.
  - › It may be advantageous to engage a partner with expertise in program development to help get a kick-start your program.
- **Process**
  - › A process for **discovery** of relevant and applicable compliance and regulatory practices is important.

  - › It is crucial to have a **repeatable** process for assessment, even if it's very basic.
  - › A repeatable qualitative reporting process is important to establish a register, and gain credibility.

- **Tools**
  - › Existing tools such as a GRC platform unless extensive work is required.
  - › Drive repeatability by developing an initial questionnaire or assessment tool, often in the form of a spreadsheet or web form.
  - › Standardize reporting templates.

Capabilities

- **Governance and Management** – Obtain a program charter with key stakeholder support, identified needs and critical asset awareness.
- **Risk Identification** – Focus on documenting and understanding critical business processes and assets to provide guidance into where to perform qualitative assessments.
- **Risk Assessment** – Define a preliminary but repeatable risk assessment capability.
- **Reporting** – Report findings qualitatively in the most convenient manner for the given stakeholder.
- **Treatment** – Share conclusions with key stakeholders to begin building a risk register without expectation of adequately addressing identified issues.
- **Monitoring** – Monitoring of remediation is out of scope at this phase.

Operational Advice

- Start with identifying key stakeholders, and among those, *champions* who have an interest in program success, to leverage them to help drive program goals "up and across" the organization. Often the key stakeholders will be corporate risk management, procurement, legal and compliance.

- It is important to focus on driving program awareness. If constituents and stakeholders don't know the program exists, even in its initial form, adoption will be minimal.

- Before starting any assessments or similar work, it is absolutely necessary to identify business-critical processes and assets, otherwise risk identification will fail to capture key areas of focus for the business.

- Keep the high-level focus on eliminating surprises – minimizing the unknown unknowns has a tremendously positive impact on the overall security state of the business and is relevant to more than just third-party risk.

Phase 2 – Opportunistic Execution

Key Outcomes

- **Program Scope** – Program scope shifts into an opportunistic mode of operation. Identify opportunities to assess what appears to be high risk known through existing relationships and previous discovery.

- **Risk Assessment** – The key outcome for assessment is successfully leveraging an industry-standard assessment framework with some potential adaptations for the type and maturity of the business. This supports development of repeatable assessment processes using industry standards, with adaptations for business-specific regulatory or compliance needs.

- **Risk Treatment** – Risk treatment is an escalation of identified high-risk issues to an un-managed remediation cycle. Essentially, risk treatment provides the capability to classify high-risk relationships, identify and request remediation from the vendor and escalate non-compliance to the line-of-business owner for remediation. This work helps establish credibility through tasks like cataloging, prioritizing and providing manageable remediation recommendations.

Components

- **People**
  - › A tasked, part-time person should be available from the enterprise security organization for program management and development.

  - Identify people from line-of-business as interaction and aggregation points for communication, tasking, etc.

- **Process**
  - Create a governance and policy framework to establish the requirement to obtain a third-party risk assessment when entering into a new engagement. The framework should be updated on an appropriate basis depending on the level of risk.
  - In conjunction with the legal team, develop contract language to be included in each contract that requires implementation of specific security controls, right to audit and breach notification. Establish Service Level Agreements for time to resolution of identified security shortfalls.
  - Develop a uniform but repeatable process for a generic third-party risk assessment.
  - Create a reporting framework with the ability to search and identify previous results, audits, etc.
  - A structured reporting process to provide risk-assessments to third parties should be available, in a repeatable and documented manner.
- **Tools**
  - Where not already present in previous steps, investigate a technology platform for program development.
  - Any tools that provide aggregation of assessment data for reporting and trending purposes are helpful.
  - Use tools (often custom-coded) that provide repeatable assessment capabilities, including self-assessment by a third party.

Capabilities

- **Governance and Management** – Utilize a process that captures third-party relationships as they are discovered and identified through existing means.

- **Risk Identification** – Determine inherent risk through a qualitative analysis process incorporating applicable external requirements, such as regulations and compliance needs.

- **Risk Assessment** – Use a primarily qualitative, one-size-fits-all process for assessment which addresses identified third parties based on highest risk potential (from identification exercise).

- **Reporting** – Provide simple fact-based reporting to key stakeholders and escalated to CISO where high-risk items arise.

- **Treatment** – Document output of qualitative analysis with recommendations for remediation; send to third party.

- **Monitoring** – Passive monitoring (opportunistic) is necessary for new third parties added through known processes and channels.

Operational Advice

- Develop strong relationships with key stakeholders such as legal, risk and vendor management to aid in program progression and alignment.

- Keeping stakeholders aware of the risks identified in a structured manner, such as a quarterly business report, is important and continues to build awareness across various stakeholder groups.

- When building an assessment tool or questionnaire, develop binary questions (yes/no/% complete) to perform automated analysis, but also allow for expanded answers to capture the respondent's complete thoughts. The questions should first determine whether the specific control is present (e.g. Data Leakage Prevention) and then dive into the maturity and scope of the deployment.

Phase 3 – Operational Development

Key Outcomes

- **Program Scope** – Program scope adapts to findings and patterns developed over the previous two phases but focuses on IT-centric data exchanges and network connections with third parties.

- **Risk Assessment** – Risk assessment adopts a stratified approach based on three tiers developed from stakeholder input.

- **Risk Treatment** – Organization adopts a managed remediation process which incorporates third-party feedback.

Components

- **People**
  - › Dedicated team of people from enterprise security to drive the program and operational activities.
  - › Engage line-of-business stakeholders who hold active accountability for driving third-party risk program.
- **Process**
  - › Business-aligned and supported process for assigning risk tiers to identified third parties.
  - › Structured, multi-tiered assessment process incorporating both remote and on-site assessment.
  - › Standardized contract language accepted into legal and vendor management processes.
- **Tools**
  - › Developing (testing) a third-party risk platform.
  - › Standardized risk assessment tool developed in a common platform utilized across business.
  - › Common reporting and visualization tool in development/testing.
  - › Remediation tracking to monitor activities to correct deficiencies in security controls.

Capabilities

- **Governance and Management** – Actively engage stakeholders who are helping drive the program and identify third-party relationships within their domains; actively maintain third party register.
- **Risk Identification** – Formula for determining inherent risk becomes quantitative based primarily on IT-related factors.
- **Risk Assessment** – Third parties are separated into tiers and assessed using a standardized and documented assessment methodology.
- **Reporting** – Assessment results are aggregated and programmatically submitted into aggregate tool or system of record, including a statement of informed opinion as analysis.

- **Treatment** – Provide remediation requirements to third parties post-assessment and validate as level of effort permits.

- **Monitoring** – Perform active monitoring of risk event notifications from identified third parties to trigger response activities.

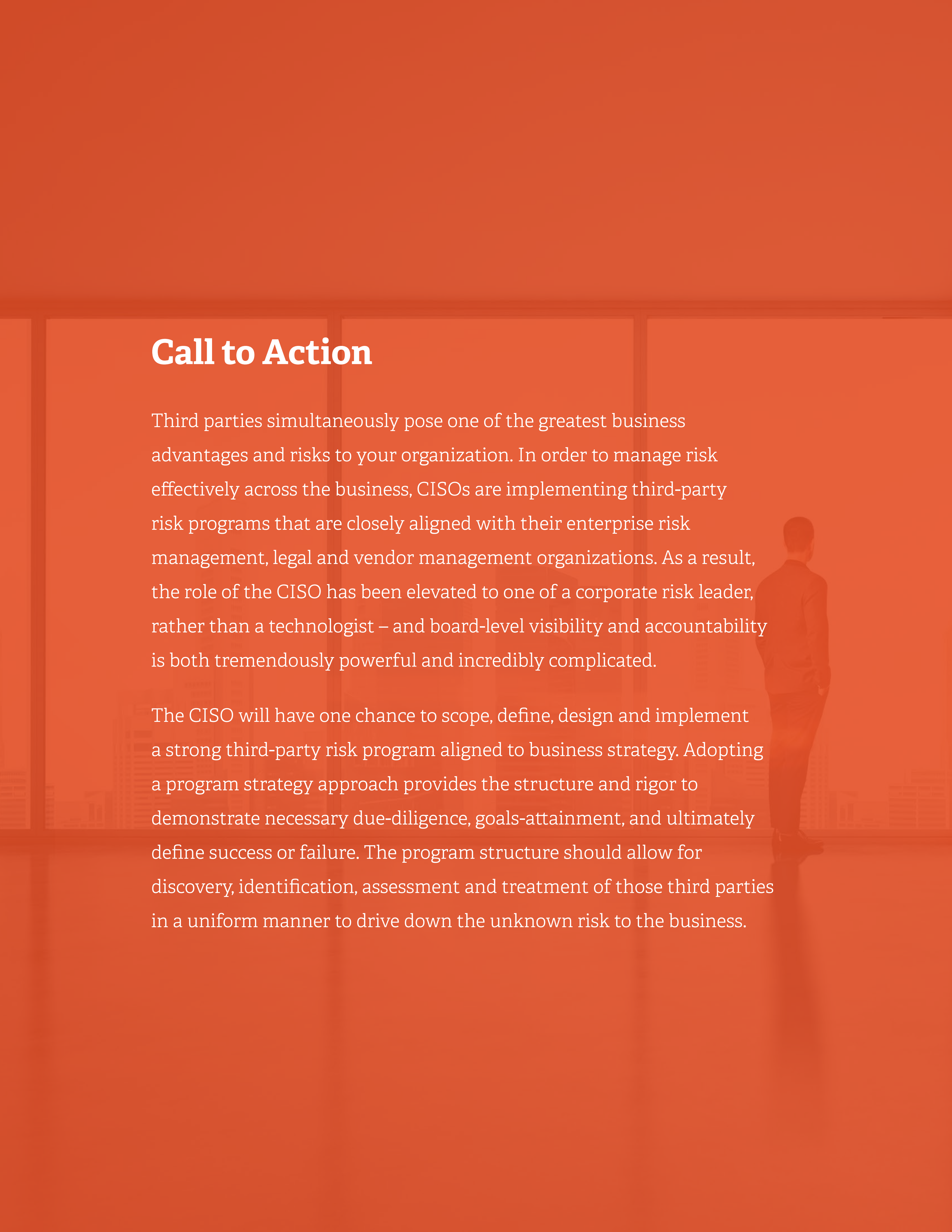
Operational Advice

- Engage business stakeholders in review and approval processes with their line-of-business third parties to drive better understanding and tighter awareness.

- Determine the “right” level of detail for reporting out to each of your key stakeholders – this will often be different depending on the person, their role and placement in the organization.

- Consistency and documentation is absolutely critical to establishing and maintaining credibility. Utilize a quality approach and train staff accordingly.

Effectively, the above phases are simply the first three levels of maturity on the overall program scale. Progressing through these first three phases provides a way to plan and execute the program strategy in manageable components. Defining with milestones and deliverables in a reasonable manner will help to demonstrate progress toward the overall business goals.



Call to Action

Third parties simultaneously pose one of the greatest business advantages and risks to your organization. In order to manage risk effectively across the business, CISOs are implementing third-party risk programs that are closely aligned with their enterprise risk management, legal and vendor management organizations. As a result, the role of the CISO has been elevated to one of a corporate risk leader, rather than a technologist – and board-level visibility and accountability is both tremendously powerful and incredibly complicated.

The CISO will have one chance to scope, define, design and implement a strong third-party risk program aligned to business strategy. Adopting a program strategy approach provides the structure and rigor to demonstrate necessary due-diligence, goals-attainment, and ultimately define success or failure. The program structure should allow for discovery, identification, assessment and treatment of those third parties in a uniform manner to drive down the unknown risk to the business.

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.