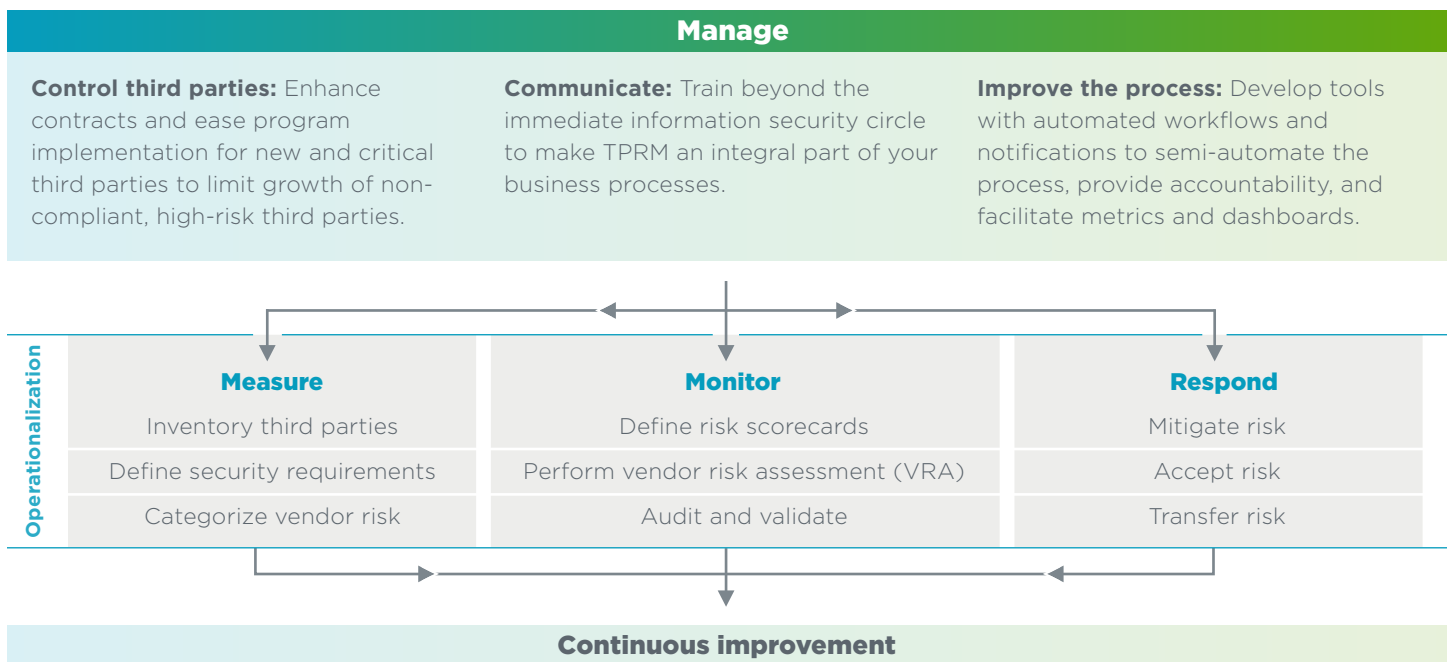# Third party risk management

Expertly manage third-party and vendor supply chain risks

Because organizations in every industry rely on third parties for business process outsourcing, measuring and managing third-party risk is mission critical. Our third party risk management (TPRM) approach provides visibility into vendor risk and strategies that manage and reduce risk. Whether we design a program for you or improve your current program, our processes provide a better way to risk stratify your vendor portfolio and appropriately manage risk across your organization.

Our approach

Our Six Sigma process improvement model helps reduce risk and minimize time impact across the third-party lifecycle, so you can focus on your core business. We help address risk management resource and skills gaps that may expose your organization to third-party risk and regulatory gaps, so you can better understand supply chain risk and meet compliance objectives. To reduce vendor "clutter," we increase attention on vendors that pose the most significant risk to your organization.

Manage

| **Control third parties:** Enhance contracts and ease program implementation for new and critical third parties to limit growth of non-compliant, high-risk third parties. | **Communicate:** Train beyond the immediate information security circle to make TPRM an integral part of your business processes. | **Improve the process:** Develop tools with automated workflows and notifications to semi-automate the process, provide accountability, and facilitate metrics and dashboards. |

Operationalization

Measure	**Monitor**	**Respond**
Inventory third parties	Define risk scorecards	Mitigate risk
Define security requirements	Perform vendor risk assessment (VRA)	Accept risk
Categorize vendor risk	Audit and validate	Transfer risk

Continuous improvement

Measure

- **Complete a full inventory:** Seek information on all third parties from procurement, accounting, international operations, and legal departments.
- **Establish security requirements for each third party:** Address company-specific requirements that service providers must meet.
- **Categorize vendor risk:** Screen third parties for a preliminary classification and document associated risk period.

Monitor

- **Operationalize procedures:** Build internal processes and scorecards to help personnel meet procedure requirements.
- **Perform a VRA:** Use the customized risk assessment questionnaire to do a "deep dive" for high- or critical-risk vendors and others as warranted.
- **Validate results:** Go beyond vendors' initial responses to identify hidden risks.

Respond

- **Mitigate risk:** Engage third parties programmatically to drive control implementation and risk reduction.
- **Accept risk:** Establish clear criteria and processes for risk acceptance, as not all risks can be mitigated.
- **Transfer risk:** As needed, transfer (via insurance or other means) some risk areas.

Comprehensive methodology

Our practitioners design required capabilities to manage risk, create new solutions, and establish operational approaches and governance models. We help you understand and manage third-party risk throughout the risk management lifecycle.

- **TPRM workshop:** Provide insights into third-party risk management and how those insights relate to your business.
- **Policy and procedure development:** Provide guidance or assistance in defining key processes to manage third-party risk.
- **VRA and classification workbook:** Classify third parties based on characteristics useful to your organization. As appropriate, we base questionnaires on applicable standards and your specific needs.
- **Training:** Provide hands-on experience in modern third-party risk and guidance for managing the entire risk management lifecycle.
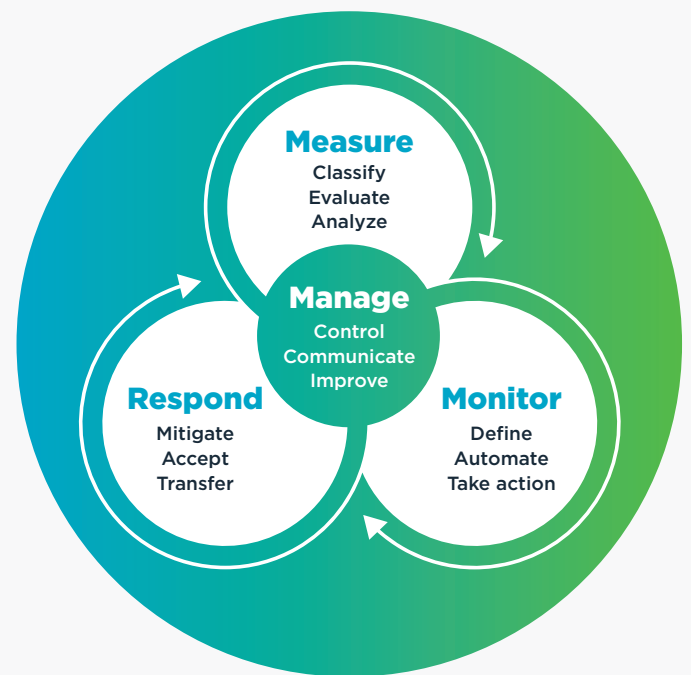
TPRM benefits

We have assessed many companies, some with thousands of third parties that access sensitive data. Our TPRM program can help you:

- Understand what third parties to include or exclude.
- Segregate your ecosystem based on criticality and perceived risk.
- Assist in risk ranking and understanding the risks in evaluating and corresponding the rating criteria.
- Develop policy and procedures to establish consistent language and processes.
- Provide a VRA framework to guide your risk evaluations and response.

Our experience

With extensive security and privacy experience across multiple industries, including payments, finance, and healthcare, our advisors can evaluate third-party risk and develop your program. We use four risk management pillars to build or update your TPRM program:

- **Measure** the risk of the activity and the vendor; tie to key systems such as ERM and ticketing, where practical.
- **Monitor** new and evolving risks, including vendor changes.
- **Respond** by using standard mechanisms (accept, decline, transfer, modify) to deal with risk.
- **Manage** using data-driven analysis to streamline and improve processes over time.

Measure
Classify
Evaluate
Analyze

Manage
Control
Communicate
Improve

Respond
Mitigate
Accept
Transfer

Monitor
Define
Automate
Take action

Mitigate third-party risk.

Learn more about Coalfire's TPRM program.
Coalfire.com | 877-224-8077

COALFIRE.

About Coalfire

The world's leading organizations – the top 5 cloud service providers; 8 of the top 10 SaaS businesses; and 3 of the top 5 in financial services, healthcare, and retail – trust Coalfire to elevate their cyber programs and secure the future of their business. As the largest global firm dedicated to cybersecurity, Coalfire delivers a full lifecycle of solutions through professional services, managed services, and technology platforms to help our clients solve their toughest cyber challenges. With more than 20 years of proven cybersecurity leadership, Coalfire combines extensive cloud expertise, industry knowledge, and innovative approaches to fuel success. For more information, visit Coalfire.com.