COALFIRE

DATASHEET

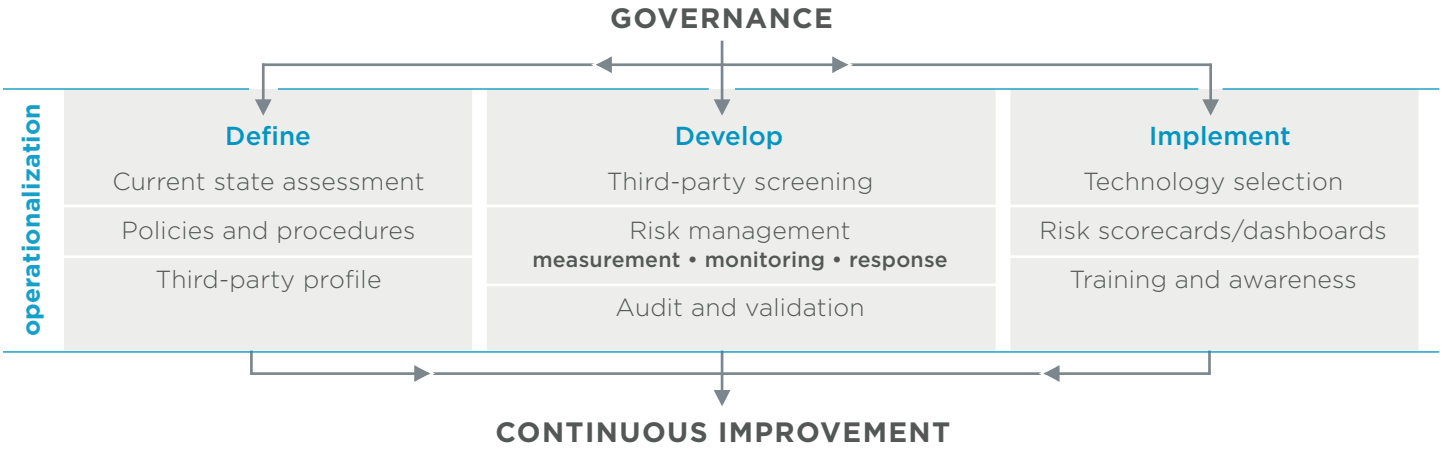
Third-party risk management support

Support third-party risk management with help from Coalfire's cybersecurity experts

All businesses rely on third-party management to effectively stay up and running. Coalfire's third-party risk management (TPRM) provides greater assurance that third-party risk is being adequately managed. TPRM draws on our knowledge of the cyber risk landscape, experience assessing and validating cybersecurity capabilities and underlying technologies, and extensive expertise evaluating security programs to help organizations assess vendor risk.

OUR APPROACH

Using a comprehensive, top-to-bottom approach, we provide key processes to manage risk across the third-party and vendor lifecycle. Our approach uses a client-centric methodology, customized to incorporate regulatory or security framework requirements relevant to your organization.



Define:

- **Develop third-party risk categorization:** Define, identify, and document risk associated with each third party.
- **Establish security requirements for each third party:** Address specific company security requirements that third-party service providers must meet.
- **Complete a full inventory:** Seek detailed information to build a complete inventory of all third parties from procurement, accounting, international operations, and legal departments.
- **Maintain a secure repository for contracts administration:** Support renewals, incident response, and legal recourse.

Develop:

- **Third-party risk screening process:** Screen existing third parties for a preliminary classification, and document the risk associated with each.
- **Operationalize procedures:** Build internal processes to help personnel meet procedure requirements.
- **Vendor risk assessment (VRA):** Use the optional CyberGRX tool or a customized risk assessment questionnaire to do a "deep dive" for high- or critical-risk vendors and others as warranted.

Implement:

- **Phase in the TPRM program:** Focus on program implementation for new and critical third parties, which allows you to ease into implementation and limit the growth of non-compliant, high-risk third parties.
- **Training and awareness:** Train beyond the immediate information security circle to make TPRM an integral part of enterprise business processes.
- **Tools development and integration (optional):** Develop tools with automated workflows and notifications to semi-automate the process, provide additional accountability, and facilitate appropriate metrics and dashboards.

COMPREHENSIVE SERVICES

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

Our TPRM offering includes:

- **Third-party risk management 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 leverage the CyberGRX TPRM service or 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:

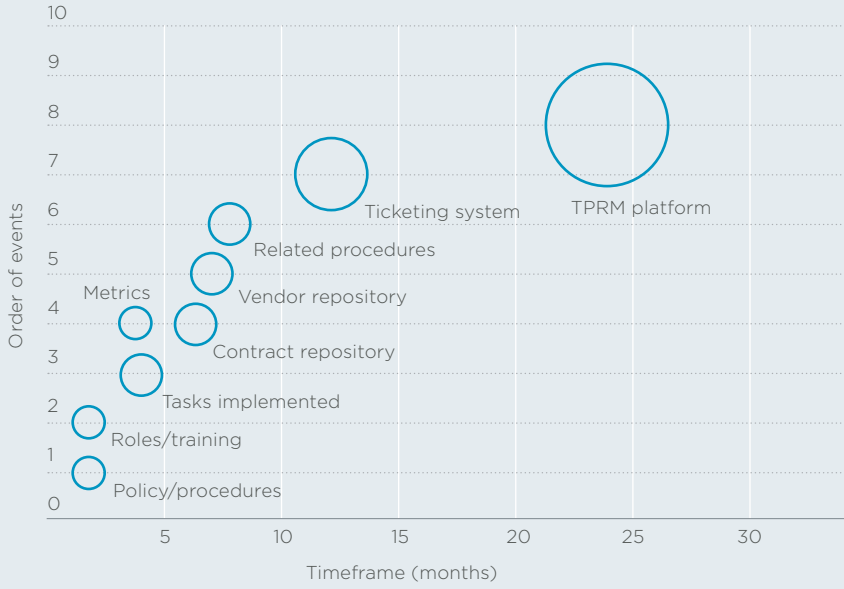
- Understand what third parties to include or exclude.
- Segregate your ecosystem based on criticality and perceived risk.
- Assist in risk ranking and understanding the risks in evaluating and corresponding the rating criteria.
- Develop policy and procedures to establish consistent language and processes.
- 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 out your TPRM program:

- **Risk management:** Use standard mechanisms (accept, decline, transfer, modify) to deal with risk.
- **Risk measurement:** Measure the risk of the activity itself and the vendor; tie to key systems such as ERM and ticketing, where practical.
- **Risk monitoring:** Monitor new and evolving risks, including vendor changes.
- **Risk response:** Respond to incidents – on behalf of the organization and vendor.

Third-party risk management example implementation roadmap



Size of bubble represents estimated relative level of effort.

MITIGATE THIRD-PARTY RISK.

Learn more about Coalfire's TPRM program.
Coalfire.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**

DS_ TPRMS_080318