Diligent

THIRD PARTY RISK MANAGEMENT

Solution Checklist

As enterprises continue to outsource more operations to third parties, they expose themselves to more shared risk. Most organizations understand the need to automate third-party risk management (TPRM) activities to ensure that they effectively manage and prevent risks. Yet many struggle to identify and prioritize the key features needed in a TPRM solution. The following solution checklist outlines key features you should look for.

Third-Party Risk Assessment Workflow

Third-party Onboarding & Centralized Third-Party Inventory

Your solution should provide a centralized repository of third-parties, and should support:

- An automated and bulk import capability for migrating third-parties into the TPRM tool.
- Integration capability for accounts payable, etc.

Corrective Action Plans

Once gaps are identified, you should be able to track and automate recommending, approving, and executing corrective action plans (CAPs). The solution should support the inclusion of third-party users in the CAP workflow by allowing them to create plans, submit them for review, and provide status updates.

Out-of-the-box Content

Whether your environment uses standardized control content like HITRUST or Shared Assessments, or general-purpose best practices like ISO, your solution should offer a content library, allowing you to get your program up and running quickly.

Out-of-the-box Classification, Assessment, & Remediation Workflows

The essential processes you need to automate are:

- The classification of third-parties into high-level "buckets," based on criticality.
- The distribution and collection of assessments, based on those criticalities.
- The identification and remediation of gaps, based on the responses to those assessments.

While every company's approach to TPRM is unique, yours isn't the first to solve for these core processes. Your solution needs to leverage industry best practices for automating the assessment process.

Third-Party Engagement

Criticality-based Assignment of Control Questionnaires

Many organizations make the mistake of asking every third-party the same questions, gathering huge amounts of data, and attempting to make sense of it. As a result, they often struggle to get valuable responses from third-parties, and they drown their staff in unnecessary paperwork.

You need short classification questionnaires for quickly identifying the high-level risks and criticalities in your third-party relationships, and targeted questionnaires that ask only what you need to know.

Risk Reporting Requirements

Dashboarding & Reporting

Your TPRM solution should come with a rich library of out-of-the-box, role-based dashboards and reports with a variety of presentation styles (e.g., third-party detail reports, list reports, charts and graphs). You should also ensure the tool lets you create, modify, and publish dashboards.

Flexible Risk Categorization and Scoring

You want your solution to provide meaningful reports showing third-party risk across all areas that are important. One thing we've learned after so many implementations across so many diverse organizations is that each one tracks its own unique risk categories, priorities, and tolerances. Make sure your system is flexible enough to accommodate what's unique to you and can grow with your organization's changing risk profiles.

Document Register

Your TPRM solution should provide the ability to track document attachments as part of a third-party profile. Attachments could include items like financial statements, incorporation filings, policies and procedures, compliance screening, and due diligence reports.

Continuous Monitoring

Third-party risk management is an ongoing process. Continuous monitoring can be accomplished in a number of ways, but a few common ones include:

- Automating the scheduling of follow-up assessments based on the risk level of a third-party. A low-risk third-party may be scheduled for re-assessment every three years, while a critical third-party may require quarterly reviews.
- Integrating third-party intelligence feeds that provide ongoing monitoring alerts for significant changes to a third-party's risk ratings (e.g., credit ratings, IT security risk ratings, new appearances in adverse media or on government watch lists).

Architecture & Infrastructure

Flexibility to Adapt to Evolving Requirements

Regulatory requirements, stakeholder expectations, and the strategic goals and risks identified by your organization will continue to change over time. The last thing you need is a rigid TPRM solution that keeps you behind the curve. Look for solutions that can quickly adapt to changes in questionnaire content, the capture of metadata, scoring and prioritization methodologies, workflow, and integrations with other systems.

Integration with Other Systems & Third-Party Intelligence

Your TPRM solution should have the ability to integrate with internal systems like LDAP, procurement, and accounts payable, as well as with third-party intelligence content. Examples include feeds that can augment your internal assessments with objective information about a third-party's IT security posture, financial viability, and compliance posture.

LEARN MORE

About Diligent™

Diligent created the modern governance movement. As the leading governance, risk and compliance (GRC) SaaS company, we serve 1 million users from over 25,000 customers around the globe. Our innovative platform gives leaders a connected view of governance, risk, compliance and ESG across their organization. Our world-changing idea is to empower leaders with the technology, insights and connections they need to drive greater impact and accountability – to lead with purpose.

For more information or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com

© 2022 Diligent Corporation. "Diligent" is a trademark of Diligent Corporation, registered in the US Patent and Trademark Office. "Diligent Boards" and the Diligent logo are trademarks of Diligent Corporation. All third-party trademarks are the property of their respective owners. All rights reserved.