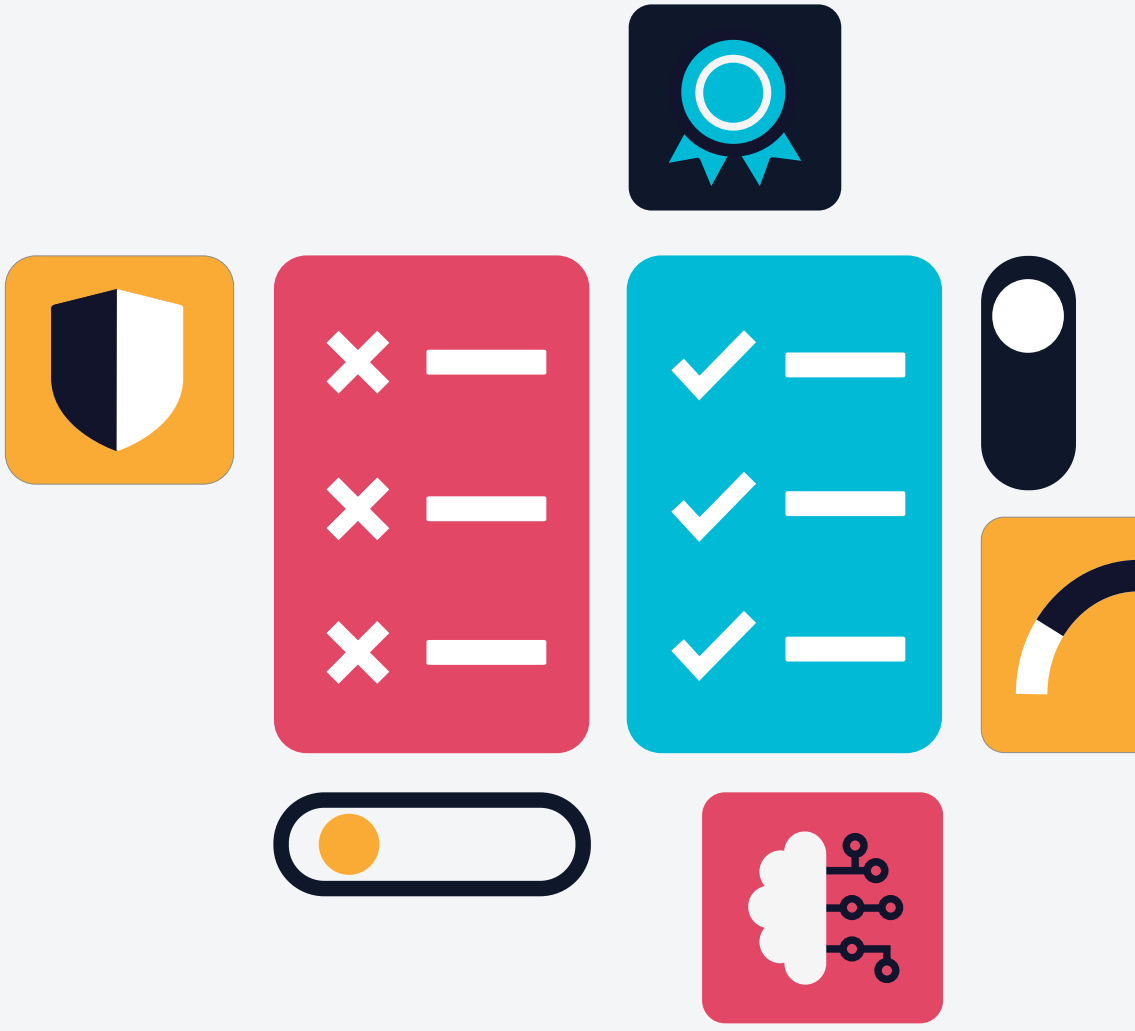
The Total TPRM Maturity Checklist

Everything You Need to Build and Benchmark a World-Class Third-Party Risk Management Program



whistic

Is Your Third-Party Risk Management Program Ready for the Future of Digital Business?

Cloud-based technologies, Artificial Intelligence, and SaaS offerings are more important to business outcomes than ever before. This leads to an increasing number of third-party relationships, which in turn means there are more access points to your critical systems, customer data, and personal identifiable information (PII).

To reap the benefits of digital transformation and innovation, your business needs a systematic plan for understanding, identifying, and mitigating the risks that can originate in your third-party ecosystem.

Third-party risk management (TPRM) should be an essential part of your cybersecurity strategy. But getting it right can be a complex challenge—in many companies, TPRM programs are ad hoc, disjointed, and highly manual. In every case, a great program involves numerous stakeholders and teams, and outcomes will affect the entire business.

Mastering that complexity is what this checklist is all about. We've broken down the TPRM process into five core pillars that work in harmony to create a mature program. Use this list as guide to benchmark your existing program to see where you stack up and identify opportunities for growth and improvement—whether it's a small tweak or a complete overhaul.

5 Core Components of a Mature TPRM Program

✔ Program Governance

Establish an oversight plan for your third-party risk management program to determine lines of accountability and communication, generate reporting for continuous improvement, and remain compliant with regulatory requirements.

✔ Policies, Standards, and Procedures

Build consistency and standardization around risk identification and assessment, mitigation and control, crisis and incident response, and vendor relationships.

✔ Vendor Risk Assessment Process

Know the risks you're taking whenever you build a third-party relationship. Understand the risk factors that most impact your business, define due diligence in the vendor selection process, and flag potential areas of concern early to properly allocate resources.

✔ Program Management

Determine the key stakeholders to include in your TPRM process, define the key performance indicators (KPIs) and metrics to track to drive success and improvement, and build transparent, consistent lines of communication.

✔ Data and Technology

Select technology solutions that enable automation, are scalable and flexible, integrate easily with the systems you use most, and create real-time reporting to track key metrics.

1 Program Governance

Governance of your third-party risk management program establishes clear lines of responsibility and accountability, ensuring there are defined roles for a diverse group of stakeholders across the organization.

Strong governance establishes oversight, accounts for regulatory compliance requirements, details lines of communication and reporting, and lays a foundation for continuous improvement. A great program also helps to maintain vendor relationships through contract management and ongoing transparency.

Create a TPRM Committee for Vendor Oversight

- Include representatives from Compliance, Legal, Procurement, IT, and business units.
- Conduct regular meetings to make strategic decisions around vendor management.

Define Metrics for Reporting to Senior Management and the Board

- Establish the most important KPIs, including things like number of vendors, risk exposure levels, compliance status, vendor performance ratings, and incident trends.
- Ensure these KPIs align with your governance structure.

Decide on Security Requirements in Vendor Contract Language

- Begin aligning contract language with industry security standards such as ISO 27001, NIST Cybersecurity Framework, and GDPR.
- Be sure to include controls for regulatory and legal requirements specific to your industry.

Document Requirements for Fourth Parties

- Identify the fourth parties that play a critical role in delivering services.
- Ensure your contracts with primary vendors include provisions for notifying you of any fourth parties they use in service delivery.
- Require primary vendors to include similar provisions in their fourth-party contracts.

2 Policy and Procedure

Policies and procedures provide a standardized and consistent approach to managing third-party risks. They create a framework for assessing, monitoring, and mitigating risk associated with vendors in your supply chain, aligning every part of your business to shared practices to reduce gaps and inconsistencies.

You should have clear policies in place for identifying and measuring risk, assigning controls for risk reduction, and planning for crises and incident response. You should also document standards for vendor relationships, including expectations for vendor performance and ongoing compliance.

Create Process to Maintain an Accurate Inventory of Vendors

- This is a centralized, accessible vendor database that catalogs essential information, including vendor names, contact details, services provided, contract details, risk ratings, and compliance status.
- Determine the data necessary to rank and categorize vendor risk, such as system access, data volume, data classification, and criticality.

Define a Tiered Vendor Classification Structure

- Establish criteria to determine if a vendor poses a High, Medium, or Low risk and develop controls tailored to each tier.
- Determine the type and frequency of risk assessments for vendors in each tier.

Develop Risk-ranking Procedures and Assign Severity Levels

- Identify impact factors of risk (such as financial implications, operational disruptions, reputational damage, or legal consequences) and likelihood factors (such as historical data, effectiveness of your controls, and vendor performance).
- Assign a weighted score to each impact factor and likelihood factor based on their severity or frequency, ensuring that your rankings provide a balanced assessment of risks that consider both high-impact, low-likelihood risks and low-impact, high-likelihood risks.
- Clearly define the attributes and characteristics of each severity level to aid in risk communication and decision-making.

3 Risk Assessment Process

The assessment process helps identify potential risks associated with engaging third parties. By conducting these evaluations, organizations can uncover risk factors including data-security vulnerabilities, compliance gaps, financial instability, operational weakness, and reputational risks.

In addition to helping to manage risk, the assessment process is critical for demonstrating due diligence, aiding in procurement and vendor selection, and building strong business relationships with the third parties you rely on.

Send Vendors the Proper Assessment Based on Risk Scores

- Depending on risk ranking for the vendor, identify the appropriate assessment questionnaire—rely on standardized questionnaires wherever possible to address the most common risks efficiently.
- Clearly explain the purpose, scope, context, and special instructions for the assessment to your vendor; detail specific areas of focus aligned to your unique business needs.
- Leverage technology solutions wherever possible to automate processes and make completing the request easier.

Identify Control Issues and Make Recommendations

- Gather information: Collect relevant information on the vendor's processes and data-handling practices from certifications, audit reports, vendor interviews, documentation, and previous assessments/incidents involving the vendor.
- Use industry best practices and standards to evaluate and benchmark vendor controls such as cybersecurity measures, data protection/retention policy, disaster recovery, and regulatory compliance.
- Develop clear and actionable recommendations based on control issues identified; ensure communication is targeted, practical, and feasible.

Develop Vendor Assessment Reports

- Clearly communicate your assessment methodology, including assessment criteria, risk-rating approach, data sources used, and evaluation steps (including interviews, on-site visits, or documentation reviews).
- Include a high-level executive summary of your findings that synthesizes the vendor's risk profile and assessment results, including overall risk rating, key findings, and control issues or vulnerabilities.

- Provide a detailed deep-dive of assessment results broken down by categories (such as cybersecurity, data protection, financial stability, compliance, and operational resilience) and accompanied by risk ranking score for each category (with accompanying graphical representations where possible).
- Detail any control issues you identified and provide specific, categorized recommendations for improvement.

Document Remediation Plans, Review with Management, and Follow Up with the Vendor

- Clearly identify issues to be remediated, including a brief description of the issue, clear objectives for your remediation efforts, such as improving data security, enhancing compliance, or strengthening operational resilience.
- Assign clear responsibilities and points of contact for each issue. Establish milestones to track progress, and build a realistic timeline for execution that accounts for complexity and available resources.

Consolidate the Results of Assessments Across Your Vendor Inventory

- Gather assessment reports for each vendor and check for consistency across reports.
- Standardize assessment data with consistent risk-ranking scoring, terminology, and criteria so you can compare vendors more easily.
- Categorize risk areas for all vendors and group similar risks and vendors together for more systematic analysis.

Determine the Frequency and Scope of Ongoing Vendor Assessments

- Organize vendors into tiers of "High," "Medium," or "Low" risk based on risk criteria (determined in previous steps); this will help you determine how often and how much to reassess.
- Consider conducting annual reassessments for low-risk vendors; semi-annual assessments for medium-risk vendors; and quarterly assessments for high-risk vendors.
- Analyze contractual agreements to identify specific clauses related to assessments so future assessments are compliant and enforceable.
- Develop a risk-assessment calendar for greater tracking, visibility, and management.

4 Program Management

The only way to manage the outcomes of your third-party risk management program is to measure results. Metrics around risk indicators, performance, and compliance—aligned to proper stakeholders across the business through transparent communication—guide informed decisions about vendor selection, contact negotiations, risk-mitigation strategies, and resource allocation.

Metrics also help to streamline communication and collaboration by providing visibility into other aspects of TPRM. They also help to establish accountability to the process.

Establish the Roles and Responsibilities for Vendor Risk Management

- Identify key stakeholders across the entire TPRM process, including a vendor management team, risk management, compliance, legal, procurement, IT, and business sponsors.
- Determine specific roles, functions, and necessary skillsets for each stakeholder.
- Complete a RACI chart of all activities. Be honest.

Report on Metrics to Understand the Progress/ Success of Your Process

- Understand your KPIs. Establish baseline metrics drawn from historical data to set realistic targets for improvement. These benchmarks should reflect your organization's risk appetite and compliance goals.
- Collect data from all relevant sources, including risk assessments, compliance reports, vendor-performance evaluations, and audit findings. Aggregate data for a comprehensive view of overall TPRM performance.
- Analyze collected data to identify trends, patterns, and areas of concern or improvement. Extrapolate actionable insights to inform decision-making.

5 Data and Technology

TPRM involves handling vast amounts of data among multiple vendors and sources. Technology solutions provide efficient data-management tools that allow organizations to centralize, store, and access all that data quickly and easily, so relevant information is always readily available for decision-making and analysis.

There are many technology options available, but there are several important aspects to consider when selecting your platform or solution. Your tool should be easy to use and adopt, scale with your growing business, integrate with other systems, and help you track important metrics.

Consider a Third-Party Risk Management Solution That Delivers a Wide Range of Tools

- Choose the right software for your needs. Identify a solution that provides vendor onboarding, risk-assessment workflows, compliance tracking, reporting capabilities, automation, and integration with other systems.
- Software creates centralized vendor information to increase visibility and collaboration for stakeholders across the process.
- Look for opportunities to automate. Assessment workflows, tasks, notifications/reminders, and escalation mechanisms for high-risk vendors can all be automated in the right solution.
- Software can allow you to customize assessment questionnaires, implement risk scoring, and monitor vendor compliance.
- Generate comprehensive reporting on vendor risk assessments, compliance status, and risk trends, customized for unique stakeholders and senior management.

Leverage External Data Sources to Identify Security Risks or Help Complete Assessments

- Subscribe to cybersecurity rating services that use data-driven methodologies to evaluate vendors based on factors such as cybersecurity practices, historical security incidents, and vulnerabilities.
- Integrate threat-intelligence feeds into your monitoring systems to receive real-time updates on emerging threats and vulnerabilities that may impact your third-party security.
- Vendor risk-intelligence platforms aggregate data from multiple sources for a comprehensive view of a vendor's risk profile.
- Industry-specific reports and public data repositories help you with threats unique to your business while helping you monitor data-breach databases and regulatory enforcement activity.

Whistic Will Help You Take the Next Big Leap in TPRM

Great third-party risk management is a team sport. Mastering this checklist requires stakeholder alignment, great people and processes, and a plan for the future.

And it might be nice to have an extra set of hands to lighten the load. That's what Whistic is for.

Whistic's dual-sided, AI-powered platform makes it fast and simple for software buyers and sellers to connect, proactively share security documentation and information, and assess vendor risks. It's the only TPRM platform you'll ever need for automation, AI-driven insights, scale, and flexibility.

The best part? Our dedicated team is here to ensure you're set up for success. We'll help you build up your TPRM program, whether you're just getting started or simply adding the finishing touches.

Get Started Today

Schedule a consultation demo catered to the unique needs of your business and let us show you the future of TPRM.

www.whistic.com