SecurityScorecard

SOLUTION GUIDE #1

A Guide to Building Your Core Third-Party Risk Management Program

Basic Diligence and the Shift to Periodic TPRM

From Chaos to Control

This playbook is your definitive guide to launching and evolving a structured Third-Party Risk Management (TPRM) program. It's designed for organizations operating at the Basic Diligence stage which is a common and practical starting point where teams rely on ad-hoc reviews and lightweight tooling to get up and running.

From this foundational starting point, there is a valuable opportunity to build greater consistency, visibility, and impact. This guide focuses on helping you progress to a Periodic TPRM approach by introducing more defined policies and workflows, and strengthening the core practices that unlock more proactive and scalable risk management over time.

> *"The supply chain vendor landscape is multiplying rapidly, and AI is accelerating the pace of threats. Are you relying on risk management practices from the 1990s?"*
>
> State of Supply Chain Cybersecurity 2026

The Intended Audience and Value

This solution guide is specifically for organizations beginning their formal TPRM journey and aiming to move from an **Basic Diligence stage** to a **Periodic TPRM stage** with a repeatable framework.

Organizations at this stage are typically defined by the following characteristics:

Area	Characteristic of Basic Diligence
Team Structure	TPRM responsibilities are fragmented and often distributed among generalist IT or Information Security professionals.
Process State	Reliance on manual and inefficient processes (e.g., spreadsheets) resulting in significant administrative burden.
Technology Use	Minimal tooling and technology adopted, leading to disjointed and incomplete risk management processes.
Primary Need	Streamline security reviews during contracting so that vendor onboarding can move forward

This stage is defined by shifting from ad-hoc security reviews during contracting to a structured, policy-driven program that utilizes vendor tiering and recurring annual assessments to maintain compliance.

Focus	Description
Maturity Goal	Establish a structured, compliance-driven program that maintains an audit paper trail through recurring assessment cycles
Target Audience	CISO, IT Leader, TPRM Lead, IT Ops
Primary Challenge	Growing backlog of manual assessments caused by a fixed number of staff trying to keep pace with a scaling vendor inventory and recurring annual review cycles
Business Outcome	Achieve audit-readiness and operational scale by replacing ad-hoc reviews with a structured program that clears assessment backlogs and accelerates onboarding.

Expected Outcomes and Impact

Establishing a risk culture

Transition from “one-off” contracting checks to a policy-driven program that ensures audit-readiness through a repeatable assessment lifecycle.

Prioritizing vendor risks

Implement vendor tiering to focus expertise on critical partners while preventing low-risk vendors from clogging the assessment pipeline.

Creating operational efficiencies

Drastically reduce “send-to-close” cycle times, allowing a fixed headcount to manage a scaling vendor inventory without increasing the backlog.

Area	Expected Outcome	Business Impact
Risk Culture & Compliance	Audit-ready infrastructure: Establishes a formal, policy-driven program with a repeatable lifecycle.	Liability and regulatory protection: Satisfies legal, insurance, and regulatory requirements while shifting documented liability to the third party.
Vendor Prioritization	Tiered risk management: Strategic categorization of partners based on business criticality.	Optimized resource allocation: Ensures high-value technical staff focus on the most critical risks instead of being buried in low-risk “noise”.
Operational Efficiency	Accelerated cycle times: Moving from months to a standard 2-week “send-to-close” window.	Scalable growth: Enables the business to manage a larger vendor inventory without increasing headcount or slowing down onboarding.

Essential TPRM Guiding Principles

As you enhance your foundational program, these three core principles should guide your initial efforts:

Define your risk governance framework

Determine which compliance standards (like SOC 2 or ISO) will be required and ensure you have an audit-ready system of record to store historical assessments.

Establish a tiering methodology

Categorize your vendor population before launching new assessments by defining what constitutes a “Critical” vs. “Low-Risk” vendor based on business impact.

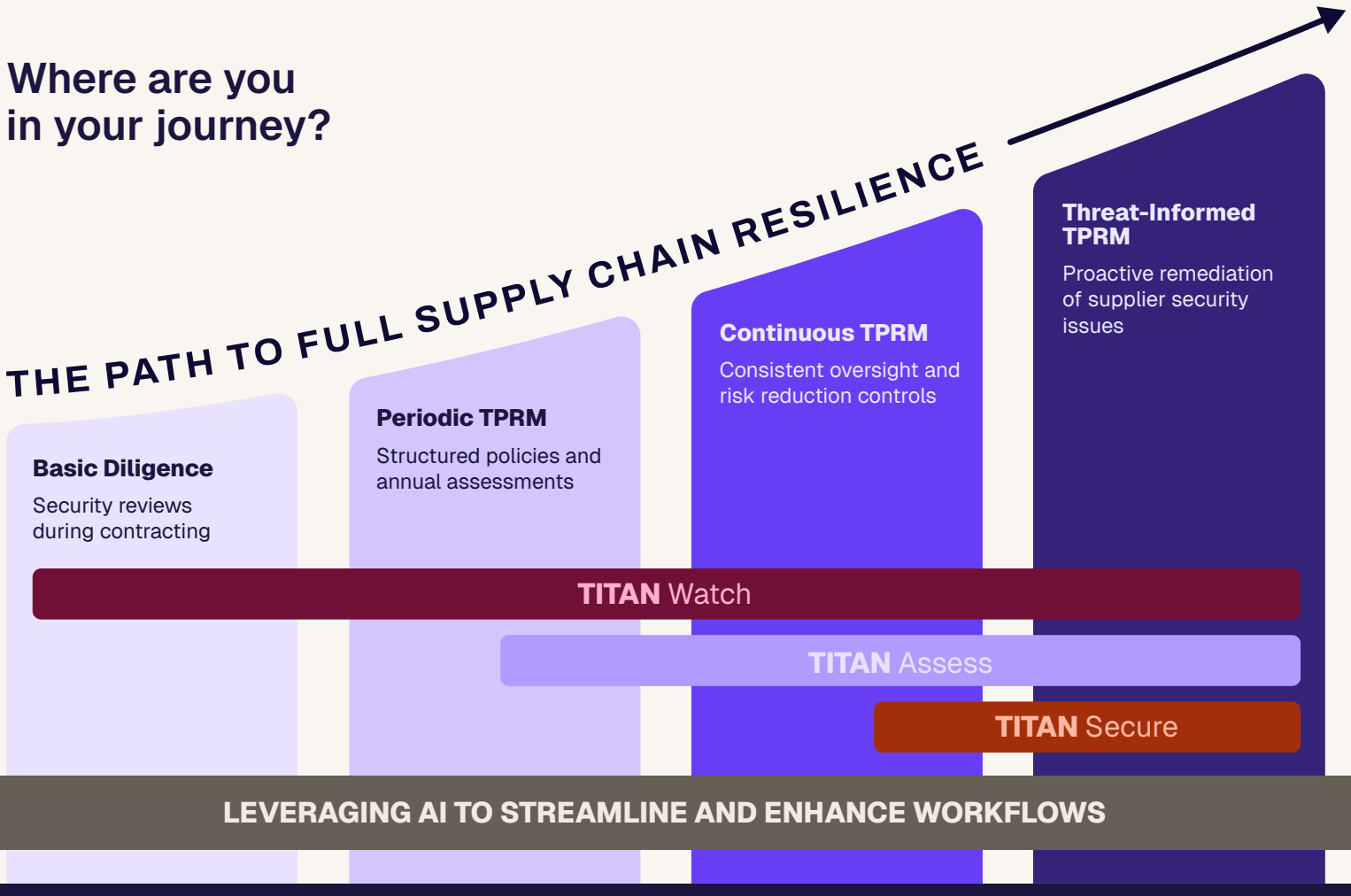
Standardize the assessment workflow

Pre-define your questionnaire sets and automated follow-up cadence to ensure you can realistically hit a 2-week cycle time as you increase your vendor coverage

DID YOU KNOW?

Research shows organizations in the Basic Diligence stage typically face questionnaire cycle times of 1 to 3 months. By implementing the tiered, policy-driven workflows in this playbook, teams compress that “send-to-close” window to just 2 weeks, an 80% reduction that accelerates the business without sacrificing security.

Where are you in your journey?



LEVERAGING AI TO STREAMLINE AND ENHANCE WORKFLOWS

Periodic TPRM: How to establish a repeatable and scalable program

This section outlines a three-step transition from manual, ad-hoc security checks to a mature Third-Party Risk Management (TPRM) program through formal governance, risk-based tiering, and standardized digital workflows.

STEP 1

Formalize Risk Governance

Transition from ad-hoc, manual security checks to a documented, repeatable program governed by a formal TPRM policy and an audit-ready system of record.

ACTION	DETAILED EXPLANATION
Draft policy documentation	Define the triggers for assessments, the types of data required (SOC 2, ISO), and the frequency of recurring reviews.
Centralize vendor data	Move vendor data from flat spreadsheets to a centralized GRC or TPRM platform to maintain a historical audit trail.
Standardize contractual language	Standardize legal language in contracts that mandates vendor participation in periodic security reviews.

BEST PRACTICE

"Audit-Backwards Mapping"

Design your assessment workflows based on what your internal auditors or insurance providers will require for proof of due diligence 12 months from now.

MATURITY MILESTONE: THE POLICY RATIFICATION

Completion is marked when the executive team approves a formal TPRM policy that mandates assessments for all vendors, not just new ones.

STEP 2

Implement Risk-Based Tiering

Resolve the operational bottleneck of "one-size-fits-all" reviews by categorizing vendors based on their potential business impact and data access.

ACTION	DETAILED EXPLANATION
Assess inherent risk	Develop a short "scoping" questionnaire for internal business owners to assess the vendor's criticality before the security review.
Assign vendor tiers	Establish 3–4 tiers (e.g., Critical, High, Medium, Low) that dictate the depth and frequency of the security assessment required.
Allocate technical resources	Assign your limited technical expertise to "Critical" vendors while using automated validation for "Low" risk tiers.

BEST PRACTICE

Contextual Scoping

Never send a questionnaire until you know if the vendor touches PII or has network access; this prevents "over-assessing" low-risk vendors.

MATURITY MILESTONE: THE CLASSIFIED INVENTORY

Completion is marked when 100% of the current vendor portfolio is assigned a risk tier, dictating their specific assessment path.

STEP 3

Standardize the Assessment Workflow

Eliminate the assessment backlog by replacing manual follow-ups with a structured “send-to-close” digital workflow.

ACTION	DETAILED EXPLANATION
Adopt industry standards	Move away from custom requirements to industry-standard sets (like SIG or CAIQ) that vendors can easily map to their existing data.
Automate follow-ups	Set up a logic-based cadence for reminders to vendors, reducing the administrative “chasing” traditionally done by staff.
Formalize exception management	Create a standard process for flagging and tracking security gaps that vendors must remediate before a “pass” is granted.

BEST PRACTICE

Slot Management

Treat your team’s bandwidth like a calendar; only allow a certain number of active assessments at once to prevent a backlog pile-up.

MATURITY MILESTONE: TWO-WEEK CYCLE TIME

Maturity is achieved when the average “send-to-close” time for a questionnaire consistently hits the 14-day mark.

KEY WORKFLOW PREVIEW

Vendor Risk Assessments

Once you have successfully transitioned from Basic Diligence to Periodic TPRM, your assessment workflow shifts from an ad-hoc manual process to a high-velocity, policy-driven engine.

PHASE	ACTION	PROCESS DETAIL
1. Intake & Tiering	**Categorize the Request**	Upon a new vendor request, the business owner completes an inherent risk intake. The system automatically assigns a Tier (Critical, High, Medium, Low) based on data access and business impact.
2. Scoped Launch	**Deploy Right-Sized Review**	Instead of a "one-size-fits-all" assessment, the a tier-specific questionnaire (e.g., a SIG Core for Critical vendors vs. a Lite version for Low-risk vendors) is triggered to reduce vendor friction.
3. Automated Outreach	**Manage the Timeline**	All follow-ups are managed via a logic-based cadence. Your team no longer "chases" vendors; automated reminders ensure the 14-day "send-to-close" target is maintained.
4. Analysis & Review	**Flag Policy Exceptions**	Technical staff only review out-of-policy responses flagged by the system. By focusing only on gaps rather than every single answer, "time-on-assessment" drops.
5. Determination	**Issue Risk Approval**	A final risk posture is generated. If critical issues exist, they are tracked in a remediation plan; if clear, the vendor is moved to the "Periodic" queue for their next annual review.
6. Audit Archiving	**Record the Snapshot**	The completed assessment and all evidence (SOC 2, ISO certs) are automatically filed in your System of Record, creating an evergreen, audit-ready paper trail for regulators.

Measurement and Next Steps

Key Metrics (KPIs) to Track

Measure progress by reporting on these business-aligned metrics:

TIME SPENT PER ASSESSMENT

Identifies the “human cost” of your program

INVENTORY TIERING COMPLETION

Ensures your risk-based methodology is actually being applied

QUESTIONNAIRE CYCLE TIME (SEND-TO-CLOSE)

Measures the speed of your assessments engine

AUDIT FINDINGS RELATED TO THIRD-PARTY RISK

Proves that you are meeting regulatory and compliance mandates

QUESTIONNAIRE RESPONSE RATE

Tracks vendor engagement and the health of your supply chain relationships

CONCLUSION

From Checkboxes to Scalable Risk Governance

By transitioning from Basic Diligence to Periodic TPRM, your organization moves beyond the “one-off” security review and establishes a defensible, policy-driven program. This shift ensures that as your vendor ecosystem grows, your risk oversight remains consistent, auditable, and operationally efficient.

The Impact of Your Progress

TARGETED RISK FOCUS

You move away from treating every vendor the same, allowing your team to focus expertise on the partners that matter most to the business.

DRASTIC EFFICIENCY GAINS

By implementing tiering and standardized workflows, you compress the “send-to-close” cycle while reducing manual review time.

CONTINUOUS AUDIT-READINESS

You replace fragmented spreadsheets with a formal system of record, creating a permanent paper trail that satisfies compliance mandates.

YOUR NEXT STEP

Shifting from Periodic to Continuous TPRM

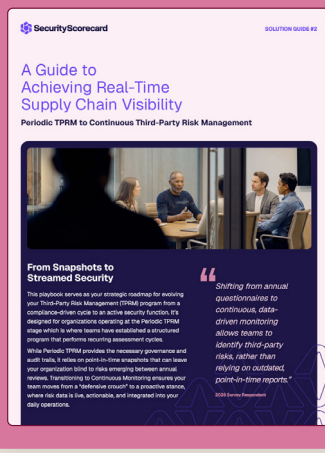
The next evolution in your journey takes you from “point-in-time” snapshots to real-time visibility. While Periodic TPRM builds the foundation of governance, Continuous TPRM ensures you are never blindsided by security regressions that occur between annual reviews.

In the next playbook, you will learn how to:

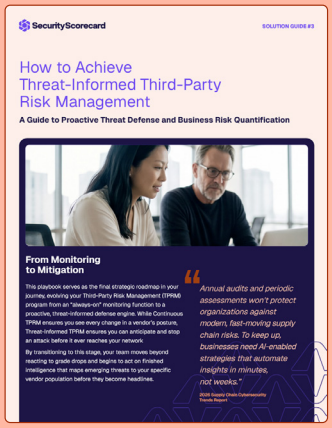
- **Close the “Visibility Gap”:** Discover how to 365-day visibility into vendor risk, moving away from the “set it and forget it” annual assessment model.
- **Scale Coverage to 100% of Your Vendor Inventory:** Learn the strategies to expand your program’s reach from a subset of critical vendors to your entire supply chain.
- **Initiate Collaborative Risk Engagement:** Learn how to activate vendor partnerships by alerting them about changes to their risk exposures, ensuring immediate accountability and remediation.

SOLUTION GUIDE #1

SOLUTION GUIDE #2



SOLUTION GUIDE #3



SecurityScorecard