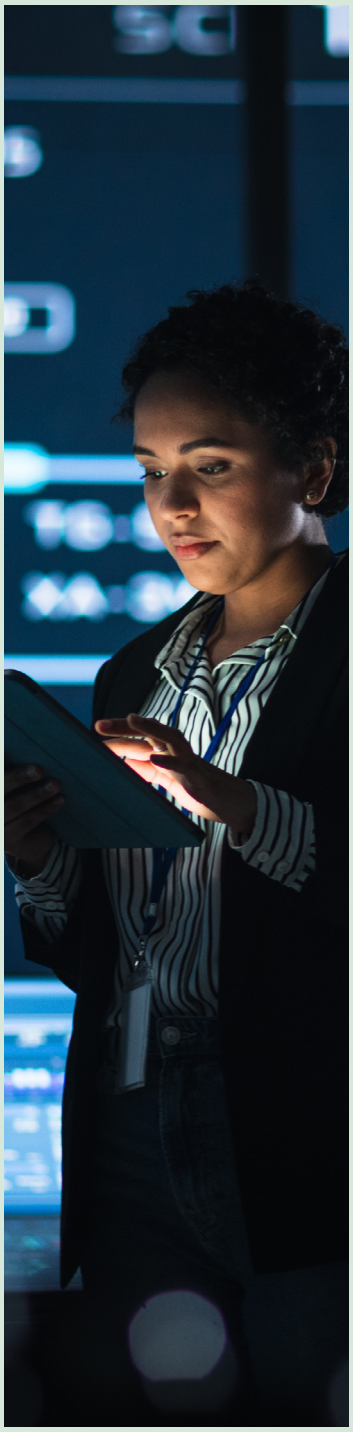
WHITEPAPER



THIRD PARTY RISK MANAGEMENT FINDING REMEDIATION: A PRACTITIONER'S GUIDE

OVERCOMING RESISTANCE, DRIVING ACCOUNTABILITY, AND CLOSING THE GAP

Abstract

Third-party risk management (TPRM) programs have matured significantly over the past decade. Organizations now assess hundreds or thousands of vendors annually, generating vast inventories of findings that require remediation. However, while assessment capabilities have advanced, the remediation process remains one of the most challenging and under-optimized areas of TPRM.

Finding remediation, the process of addressing identified risks, control gaps, and compliance deficiencies in third-party environments, is where risk reduction occurs. Without effective remediation, assessments become compliance nightmares, findings are documented but never resolved, and **residual risk accumulates silently** across the vendor portfolio.

This guide provides a practitioner-focused framework for accelerating remediation timelines, improving vendor collaboration, building scalable tracking mechanisms, and demonstrating measurable risk reduction to leadership and regulators alike.

Infosys
Navigate your next

Executive Summary

Supply chain cybersecurity programs have matured significantly in their ability to assess and identify risk. Yet the most persistent failure point is not discovery, **it is remediation**.

Four structural problems sit at the center of this failure:

1 Vendors do not want to remediate third-party audit findings

They view them as externally imposed obligations with unclear value, and resistance manifests as disputes, delays, and superficial fixes.

2 Tracking open findings is extremely difficult

Fragmented systems, lack of resources, inconsistent data, and the absence of a shared single source of truth mean findings fall through the cracks, for both–the organization and its vendors.

3 Exception management and risk acceptance become the easy way out

When remediation is hard and tracking is unreliable, the most expedient path is to accept the risk and closing the finding on paper without resolving the underlying vulnerability.

4 Standardized risk ratings drive SLAs that are disconnected from real-world threat exposure

Vendors facing multiple "Critical" findings under compressed timelines lack guidance on which to fix first; and the rigidity of the rating system undermines both credibility and compliance.

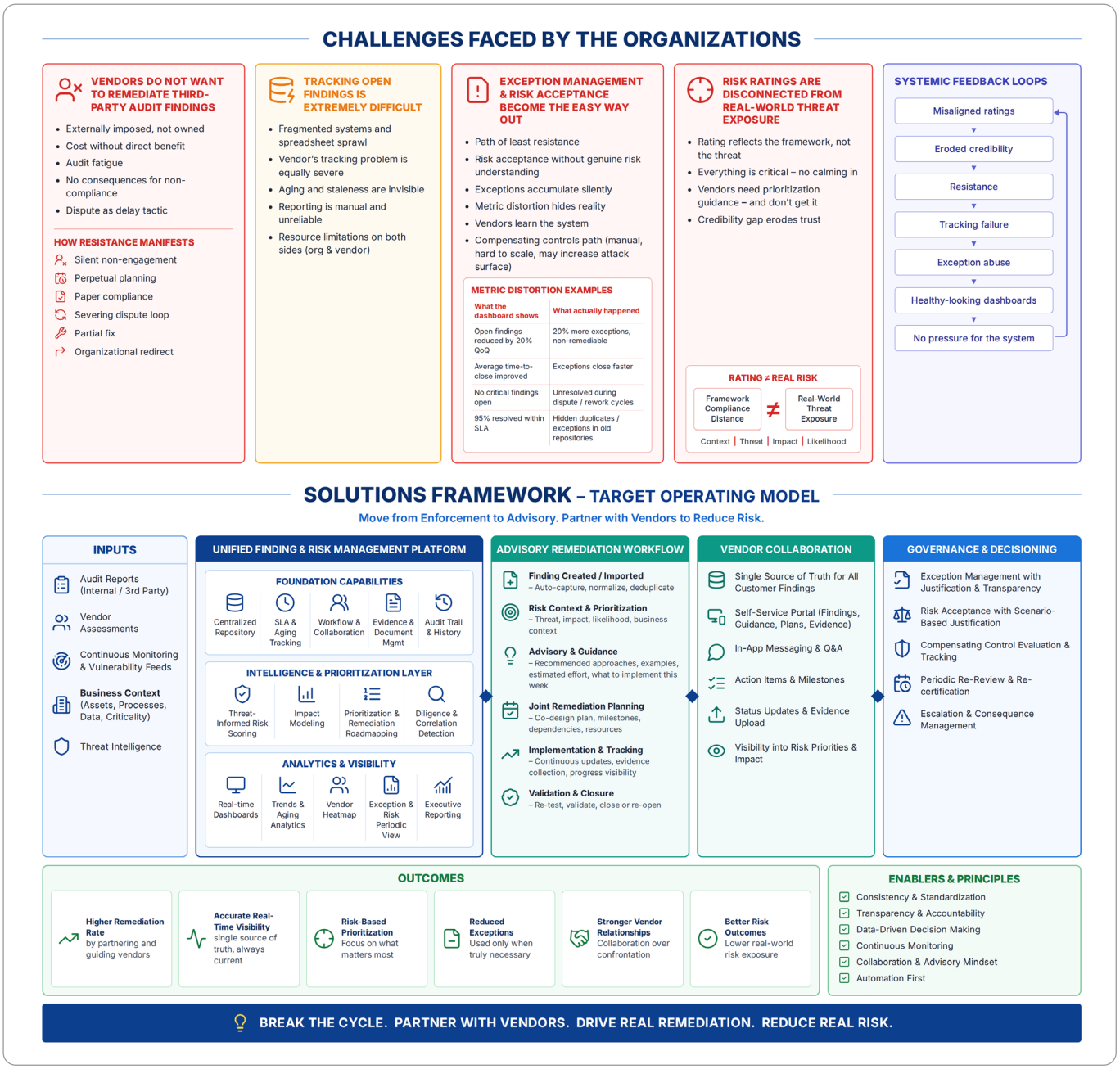
These problems form a reinforcing system. This whitepaper dissects each challenge and presents a comprehensive solutions framework built on operational principles; designed to break the cycle not by adding more processes, but by redesigning incentives, tooling, governance, and the vendor relationship model.



External Document © 2026 Infosys Limited

Architecture Diagram

This diagram summarizes the challenges faced by an organization while working with its vendors in remediating the risks and provides an overview of the solutions/best practices that can be adopted.



In the subsequent sections, we will deep dive into these challenges and solutions.

External Document © 2026 Infosys Limited

Challenges Faced by the Organizations

1: Vendor's resistance to third-party audit remediation

Vendor resistance to remediation is not irrational. From the vendor's perspective, several factors make it unappealing:

1.1 Findings feel externally imposed, not internally owned

When a third-party assessor sponsored by the customer, not the vendor, identifies a finding, the vendor perceives it as an external mandate rather than an internal priority. The finding was not surfaced by their own risk assessment process; it was imposed by someone else's framework, against someone else's risk appetite.

1.2 Cost without direct benefit

Remediation costs money, engineering time, tooling changes, and architecture rework.

For the vendor, this cost reduces the *customer's* risk, not their own. Unless the finding directly threatens the vendor's own operations, the ROI calculation seems unfavorable.

1.3 Audit fatigue

Large vendors face numerous separate audits per year from different clients, each generating its own findings—sometimes contradictory. The cumulative burden creates cynicism: "**We can't fix everything for everyone, so we fix the minimum for each.**"

1.4 No consequences for non-compliance

The vendor continues to receive purchase orders regardless of open findings. When non-compliance carries no commercial pain, remediation becomes **optional**.

1.5 Dispute as a delay tactic

Disputing severity or applicability pauses the SLA clock; buying time without formal non-compliance.

How Resistance Manifests

Resistance pattern	What it looks like
Silent non-engagement	No treatment plan submitted; emails unanswered
Perpetual planning	Treatment plan submitted but target dates slip repeatedly
Paper compliance	Policy document updated; no technical implementation
Severity dispute loop	Finding validity/applicability challenged on technical grounds
Partial fix	Easiest element addressed; root cause untouched
Organizational redirect	"That system is managed by our subcontractor"

External Document © 2026 Infosys Limited

2: Tracking open findings is extremely difficult

2.1 Fragmented systems and spreadsheet sprawl

Findings live in spreadsheets, **email threads**, GRC tools, and PDF reports. No single system holds the complete current state.

2.2 The vendor's tracking problem is equally severe

A vendor assessed by multiple customers receives findings in different formats, through different channels, and with different SLA expectations.

2.3 Aging and staleness are invisible

Without **automated SLA tracking**, findings go stale without anyone noticing.

2.4 Reporting to leadership is manual and unreliable

Dashboards require **manual assembly from fragmented sources**, thereby producing snapshots outdated by the time they're presented.

2.5. Resources limitation

Organizations often lack resources to track and chase vendor findings. Similarly, vendors lack resources to implement remedial action.

3: Exception management and risk acceptance become the easy way out

3.1 The exception as path of least resistance

An exception requires a form and a signature. Remediation requires months of sustained effort.

3.2 Risk acceptance without genuine risk understanding

Approvers see a severity label, not a scenario-based impact analysis. Risk acceptance becomes bureaucratic formality.

3.3 Exceptions accumulate silently

Once granted, exceptions are **rarely re-examined** with rigor. The portfolio of accepted risk grows unchecked.

3.4 Metric distortion

What the dashboard shows	What actually happened
Open findings reduced by 30% QoQ	20% were exceptions, 10% were remediated
Average time-to-close improved	Exceptions close faster than remediations
No "Critical" findings open	3 were downgraded during dispute; 2 were risk-accepted
95% of findings resolved within SLA	"Resolved" includes exceptions and risk acceptances

External Document © 2026 Infosys Limited

3.5 The vendor learns the system

Vendors observe that resistance leads to exceptions, not consequences. Resistance becomes self-reinforcing.

3.6 Compensating controls path

Compensating controls become the next easier way out. Instead of implementing the full controls, partial or compensating controls are implemented. Most of the time, these compensating controls bring in manual reliance (prone to errors), that are difficult to scale and may increase the attack surface.

4: Risk ratings are disconnected from real-world threat exposure

4.1 The rating reflects the framework, not the threat

Ratings measure compliance distance from a control baseline, not actual exploitability, or business impact in context.

4.2 Everything is critical, so nothing is

A vendor receiving 15 critical findings cannot remediate all 15 within a 15-day SLA. Uniform urgency is operationally equivalent to no prioritization.

4.3 Why vendors struggle: the absence of actionable prioritization guidance

Programs provide severity labels and SLA deadlines. They do not provide threat-informed prioritization, impact-weighted ranking, or remediation sequencing.

4.4 The credibility gap

When ratings do not match the vendor's understanding of their environment, every finding becomes suspect.

How these challenges form a system

The four challenges create reinforcing feedback loops:

Misaligned ratings → Eroded credibility → Resistance → Tracking failure → Exception abuse → Healthy-looking dashboards → No pressure to fix the system.

Breaking this cycle requires intervening at all four points simultaneously.



External Document © 2026 Infosys Limited

Recommended Solutions Framework

The advisory model: stop sitting on the fence, work with the vendor.

The single most important shift: **stop sitting on the fence**. Provide **advisory and consultation on remediation** along with audit findings and enforcement.

Enforcement model (Current)	Advisory model (Target)
"Remediate within 15 days."	"Here's how similar environments have solved this—two options, estimated effort, and what to implement this week."
Deliver finding list. Wait. Chase.	Joint remediation planning session. Co-design the approach.
Escalate when SLA breaches.	Proactively check in: "Do you need guidance? Dependencies we can unblock?"
Assessor leaves after report.	Advisory team stays engaged through the remediation lifecycle.

The advisory model requires the organization to have "skin in the game." Remediation cannot be expected based solely on deadlines. A dedicated Remediation team, possessing higher skills compared to the Assessment team, is essential to drive effective outcomes.

Key components:

- Remediation guidance attached to every finding.
- Joint remediation planning sessions for strategic vendors.

Advisory **does not replace accountability, it complements it**. The right to escalate is earned by first offering to help.

Leverage the relationship manager

Vendors listen to Relationship Managers (RM) more than cybersecurity teams, because the RM controls the commercial relationship.

- **Build rapport before you need it**
  Quarterly 1-page security briefings for RMs. Speak their language (supply continuity risk, not CVEs).
- **Keep RMs informed proactively**
  Never let an RM be surprised by a cybersecurity escalation.
- **Involve RMs in difficult situations**
  Non-responsive vendor? Ask the RM to open the door. Vendor disputing everything? RM reinforces importance at the next commercial touchpoint.

Relationship Managers are not expected to become cybersecurity experts; rather, they play a critical role in **leveraging their existing relationships and access** that cybersecurity teams may not be able to achieve independently.

External Document © 2026 Infosys Limited

Treatment plans with milestones—not just remediation dates

Target dates provide limited visibility into progress until **deadlines are missed**. Demand a **Treatment Plan** with:

- Root cause analysis
- Remediation approach
- 3–6 milestones with deliverables, owners, and dates
- Interim mitigation

Track milestones alongside findings in the system of record, not in separate spreadsheets.

Weekly closure reporting creates a drumbeat of accountability: findings closed, milestones completed, milestones overdue, stale findings flagged, and upcoming milestones.

Do not fall back to risk acceptance

The real value of TPRM is ensuring vendors have no open findings and have implemented the necessary security controls, thereby raising their security maturity. Risk acceptance is the opposite: every acceptance is an admission of the program failed to achieve its purpose for that finding.

True Remediation Rate *= Findings closed through verified technical remediation ÷ Total findings issued.*

This metric **excludes risk acceptances**.
Set a target. Publish it. Report against it.

Before approving any risk acceptance, a **failed remediation narrative** is required: What was attempted? Why did it fail? What advisory support was provided? If the program fails to demonstrate the genuine attempt, the risk acceptance is premature.

Prioritize findings based on the current threat landscape

Static ratings do not adapt to what adversaries are doing.

The COVID example

Before March 2020, weak VPN authentication was one finding among many. After the shift to remote work, it became the single most exploitable vulnerability in the vendor's environment. **MFA for remote access had to be prioritized above all other findings, not because the framework changed, but because the threat landscape demanded it**.

Operationalize this with a threat-informed priority override

3–5 finding categories elevated above standard ratings due to active threat conditions, updated quarterly, and communicated to all vendors. For e.g.: An unpatched server is a critical but common finding. However, when an unpatched DNS Server is being actively targeted by a prevalent ransomware group, this finding becomes top priority for mitigation.

Map findings to kill chains

A vendor who can only fix 3 things this quarter should fix Multifactor Authentication [MFA] (initial access), Privileged Access Management [PAM] (credential escalation), and backup immutability (ransomware impact); because those map to the most likely attack sequence.

Agentic AI for follow-ups—human experts for validation

Automate the chase, humanize the judgment.

AI agents handle follow-up communications, milestone reminders, overdue notifications, weekly report generation, Treatment Plan pre-screening, vendor communication drafting, and dashboard maintenance.

Human experts handle evidence validation, advisory sessions, risk judgment, escalation decisions, and vendor relationships.

External Document © 2026 Infosys Limited

Evidence-driven closure

No finding is closed without validated evidence.

A vendor email saying "we implemented MFA" is not a closure. A screenshot or demo of the MFA enforcement is the closure.

Define evidence requirements **per finding category**, publish them upfront, and enforce without exception.

Write findings objectively with clear remediation instructions

Vague findings produce vague remediations.

❌ **Vague**: "Vendor is required to create an Incident Response Plan."

✅ **Prescriptive**: "Vendor is required to create an Incident Response Plan. The Plan document should contain sections with the below requirements:

- The plan should have been reviewed and approved in the last 12 months
- Purpose, scope and objective
- Roles and responsibilities
- Incident classification and severity levels
- Incident response lifecyle
- Co-ordination with third parties
- Regulatory and legal considerations
- Incident response capability testing (and frequency)

Governance and reporting: Hold the program accountable too

The program cannot demand responsiveness from vendors while being unresponsive itself.

Three governance commitments:

Commitment	Internal SLA
Evidence reviewed promptly	Critical: 3 days; High: 5 days; Medium/Low: 10 days
Vendor emails answered	Clarifications: 2 days; Blocker notifications: 2 days
Escalations followed to closure	Acknowledged in 3 days: resolved or re-escalated within 10 days

Track internal governance on a dashboard alongside vendor performance. Present both to the senior stakeholders and leadership: "We hold the vendors accountable, **and we hold ourselves accountable.**"

Build a single system of record

- All findings from all sources in one platform with unique IDs and full audit trail.
- Vendor portal for direct view, submission, and evidence upload.
- Automated SLA tracking and escalation notifications.
- Executive dashboards that separate remediation from exceptions.

External Document © 2026 Infosys Limited

Implementation Roadmap

Phase 1 — Foundation (Months 1–3)

- Deploy single system of record and migrate existing findings.
- Define normalized taxonomy and severity mapping.
- Establish vendor portal with basic view/ submit capability.
- Brief Relationship Managers in advance.
- Implement automated SLA tracking and escalation notifications.
- Publish the consequence ladder and communicate to all vendors.

Phase 2 — Intelligence Layer (Months 4–6)

- Develop context-aware rating model.
- Build prioritized remediation roadmap templates.
- Pilot with 5–10 strategic vendors.
- Implement exception governance reforms.
- Separate remediation and exception metrics on dashboards.

Phase 3 — Partnership Model (Months 7–12)

- Launch joint remediation workshops for strategic vendors.
- Integrate Threat Intelligence into quarterly rating reviews.
- Implement Vendor Security Scorecard tied to commercial outcomes.
- Roll out complexity-tiered SLAs.
- Establish remediation playbooks for top 10 finding categories.
- Deploy Agentic AI for follow-up automation.

Phase 4 — Maturity (Months 12–18)

- Assess program metrics against baseline.
- Extend portal for cross-customer finding consolidation.
- Automate context-layer scoring using asset inventory and threat feeds.
- Recognize and reward top-performing vendors.
- Publish True Remediation Rates as the program's north-star metric.

External Document © 2026 Infosys Limited

Conclusion: Vendor Risk is Our Risk

The value of any Third-Party Risk Management program does not come from conducting many assessments or clearing backlogs. It comes from **mitigating the actual risk that an organization faces while doing business with the vendor**.

Simply put: **Vendor risk is our risk.**

A ransomware attack that takes down a vendor's production line is not the vendor's problem alone; it is a disruption to the organization's supply chain. A data breach at a vendor that exposes design files is not the vendor's incident alone; it is the organization's intellectual property at stake.

Every open finding represents a door that an adversary could walk through. The question the program must answer is not "How many findings did we close?" but "**How many doors did we actually shut?**"

This whitepaper has presented a framework for closing them effectively; not through harder mandates and bigger spreadsheets, but through advisory partnership, operational discipline, intelligent prioritization, rigorous evidence standards, and a relentless commitment to actual remediation over administrative convenience.

The program's success should be measured by one question: **Is our vendor base more secure today than it was a year ago?**

If the answer is yes: fewer findings, lower severity, faster remediation, no recurrence—the program is delivering its core value.

If the answer is no: same findings, same resistance, same exceptions—the program is running in place.

Assessments identify risk. Only remediation reduces it. Everything else is process.



External Document © 2026 Infosys Limited

About the Author



Gaurav Negi

Principal Consultant, Infosys

Gaurav Negi has 24+ years of experience across industries in the areas of Information Security Implementation and Consulting, which includes Program Compliance Management, Information Risk Lifecycle Management, and Implementation of e-GRC Framework/ Tools. Gaurav has worked with clients on SOX Compliance, ISO 27001 Implementation, eGRC Tool Implementation, and Third Party Risk Management. Gaurav possesses industry certifications like "SABSA Chartered Security Architect – Foundation Certificate (SCF)" and "Certified Information Systems Auditor (C.I.S.A)".

For more information, contact askus@infosys.com

Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.