

COMPARISON CHART

# Comparison Chart: Compliance-Only vs. Proactive TPRM Programs

## THIRD PARTY RISK MANAGEMENT

Third-Party Risk Management (TPRM) is critical for organizations to ensure their supply chain and vendor ecosystem are secure and resilient. While compliance-only TPRM programs focus

on meeting regulatory requirements, proactive TPRM programs adopt a broader, risk-focused approach that meets compliance and enhances organizational resilience.

The following chart highlights the key differences between the two approaches to help organizations make informed decisions.

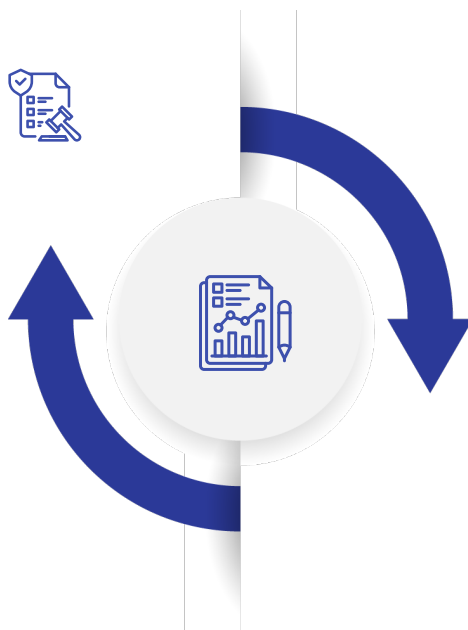
Compliance-Only TPRM Program		Proactive TPRM Program
Meeting regulatory requirements and standards	 Focus	Identifying, assessing, and mitigating risks
Periodic assessments, often annually	 Risk Assessment Frequency	Continuous, real-time monitoring and assessment
Limited to initial due diligence	 Vendor Evaluation	Comprehensive evaluation, including ongoing reviews
Reactive, often driven by compliance violations	 Response to Incidents	Proactive incident response plans, including scenario planning
Minimal engagement, mainly at onboarding	 Engagement with Vendors	Ongoing collaboration, regular communication, and updates
Minimal technology integration	 Technology Use	Utilizes automation and advanced analytics for monitoring
Basic compliance reports	 Reporting	Detailed risk reports, including trends and insights
Rigid, focused on existing regulations	 Adaptability	Agile, able to adapt to emerging threats and risks
Avoid penalties and fines	 Overall Goal	Build a resilient supply chain and enhance overall security posture
Compliance-focused training sessions	 Employee Training	Comprehensive training that emphasizes risk awareness and management

# Summary

## Compliance-Only TPRM Program



These programs focus on meeting regulatory requirements. While they ensure organizations avoid penalties, they often lead to a check-the-box approach, leaving gaps in risk management and missing opportunities to strengthen vendor ecosystems.



## Proactive TPRM Program

Proactive programs provide a holistic approach to managing third-party risks. They build resilience by leveraging technology, continuous monitoring, and vendor collaboration, enabling organizations to respond effectively to emerging threats and regulatory changes.

# Recommendations

1

### Adopt a Proactive Approach

Transition from compliance-only practices to a proactive TPRM model to safeguard against dynamic risks and build stronger vendor relationships.

2

### Train for Risk Awareness

Expand employee training to include risk awareness and management, ensuring teams can handle emerging challenges.

3

### Leverage Technology

Use advanced analytics and automation to streamline processes, enhance real-time monitoring, and gain actionable insights.

4

### Increase Vendor Collaboration

Engage vendors in regular assessments, scenario planning, and communication to build trust and shared responsibility.

5

### Prepare for the Future

Design flexible TPRM programs that adapt to regulatory changes and emerging risks, ensuring long-term security and, compliance.

# About NuSummit Cybersecurity

**NuSummit Cybersecurity** helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at [cybersecurity.nusummit.com](https://cybersecurity.nusummit.com) or write to us at [cybersales@nusummit.com](mailto:cybersales@nusummit.com)

**Dallas | Jersey City | Cupertino | Ottawa | Riyadh | Dubai  
Mumbai | New Delhi | Bangalore**

---

© NuSummit Cybersecurity Limited. All rights reserved.

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

Follow us at:   