



SAFE ONE

Third-Party Risk Management (TPRM)

AUTOMATE, UNIFY, AND
RUN YOUR TPRM PROGRAM AT SCALE



SAFE Transforms the TPRM Game

SAFE TPRM is the industry's first AI-powered third-party risk management solution, equipping businesses with the benefits of outside-in security ratings, questionnaire-based assessments, zero-trust, and inside-out assessments. Using SAFE One's unified platform, enterprises can finally obtain holistic, realistic, dynamic, and dollar-driven insights into their supply chain risk posture.

SAFE TPRM solution represents a major shift in how third-party cybersecurity risks are measured and managed. Unlike traditional methods, which provide a piecemeal view with static data, SAFE TPRM integrates diverse risk indicators into a single, clear perspective. This integration allows businesses to see not just snapshots but a continuous, real-time view of their entire third-party ecosystem.

With SAFE TPRM, companies can proactively identify and address vulnerabilities and other security findings before they become critical threats. This means businesses can better protect themselves while also making smarter, more informed decisions with:

- Risk-based Third-party Tiering
- Unified Third-Party Cyber Risk Management
- AI-Driven Automation and Insights
- Defensible, Open Standards
- Reduced Total Cost of Ownership





Solution Highlights

01 | Risk-based TPRM

SAFE TPRM calculates the financial risk and breach likelihood of cyber risk scenarios that could impact an enterprise based on their supply chain data access, network access, and resultant business interruption. This enables CISOs to tier their most critical vendors based on loss exposure instead of values such as size or revenue. By quantifying the potential dollar risk and breach probabilities, SAFE TPRM provides a clear, financial basis for prioritizing third-party risks.

This enables a more strategic allocation of resources, directing attention to the vendors that pose the greatest threat to financial stability and operational continuity. Furthermore, SAFE TPRM delivers prioritized, ROI-driven recommendations. These actionable insights guide businesses in working effectively with vendors to address and reduce cybersecurity vulnerabilities, ensuring investments in security yield measurable risk reductions.

The platform also enhances decision-making with out-of-the-box (OOTB) dashboards and reports that not only answer critical questions about which third parties pose the highest financial risk but also enable a focused approach on the most crucial vendors.

The screenshot displays the 'Organizations' dashboard in the SAFE TPRM platform. It is divided into three main sections:

- Worst Performing by Loss Magnitude:** A table showing vendors with the highest potential financial impact.

NAME	LOSS MAGNITUDE
epic	\$85.5M
Palo Alto Networks	\$51.2M
tesla	\$3.4M
- Worst Performing by Likelihood:** A chart showing vendors with the highest probability of a breach.

NAME	LIKELIHOOD
tesla	48%
Third Party Risk Association	45%
Wipro	37%
- Organization List:** A table providing a comprehensive overview of all vendors, including their risk tier, loss magnitude, and coverage status.

NAME	STATUS	RISK TIER	LOSS MAGNITUDE	COVERAGE	MANAGE
Dominos	Contingent Approved	Tier 4	\$907K	⊙ ⊙ ⊙	...
epic	Under Review	Tier 1	\$85.5M	⊙ ⊙ ⊙	...
Palo Alto Networks	Under Review	Tier 1	\$51.2M	⊙ ⊙ ⊙	...
Perplexity AI	Approved	Tier 4	\$1.4M	⊙ ⊙ ⊙	...
tesla	Under Review	Tier 1	\$509.9M	⊙ ⊙ ⊙	...
Third Party Risk Association	Under Review	Tier 4	\$974K	⊙ ⊙ ⊙	...
Wipro	Rejected	Tier 2	\$43.7M	⊙ ⊙ ⊙	...
Workday	Under review	Tier 5	\$499K	⊙ ⊙ ⊙	...

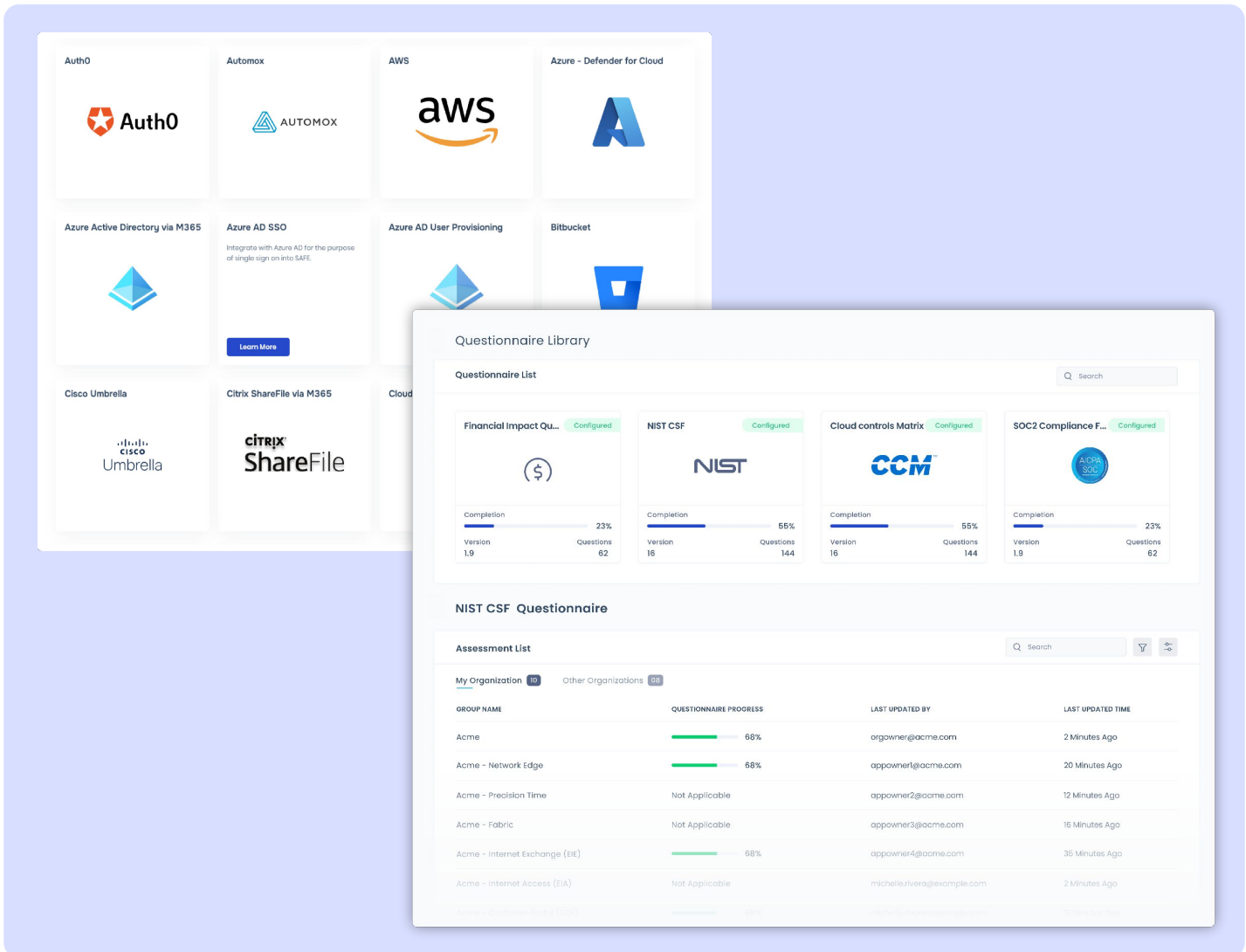


02 | AI-Driven Automation to Scale and Build Your Program

SAFE TPRM leverages AI-driven automation to radically transform and streamline the process of managing third-party risks. By automating critical components such as data ingestion, security assessments, compliance certifications and questionnaires, SAFE TPRM shifts the paradigm from traditional, disjointed, and manual practices to a cohesive, automated, and continuously updated TPRM strategy.

This automation enables businesses to handle vast amounts of data efficiently. Through telemetry automation, SAFE TPRM captures real-time data from various sources, including direct feeds from security tools. This is complemented by automated threat intelligence feeds that enrich the context and provide deeper insights into potential risks third parties pose. Additionally, SAFE TPRM simplifies the complex process of managing questionnaires. Instead of manually processing these documents, the platform automates their ingestion and analysis, pulling essential data into the system from a comprehensive marketplace that covers a wide range of security standards and industry requirements.

The result is a dynamic system that offers real-time, prioritized insights into third-party risks. This level of automation speeds up the risk assessment process, enhances accuracy, reduces human error, and allows TPRM teams to focus on higher-level strategy and intervention rather than getting bogged down in administrative tasks.



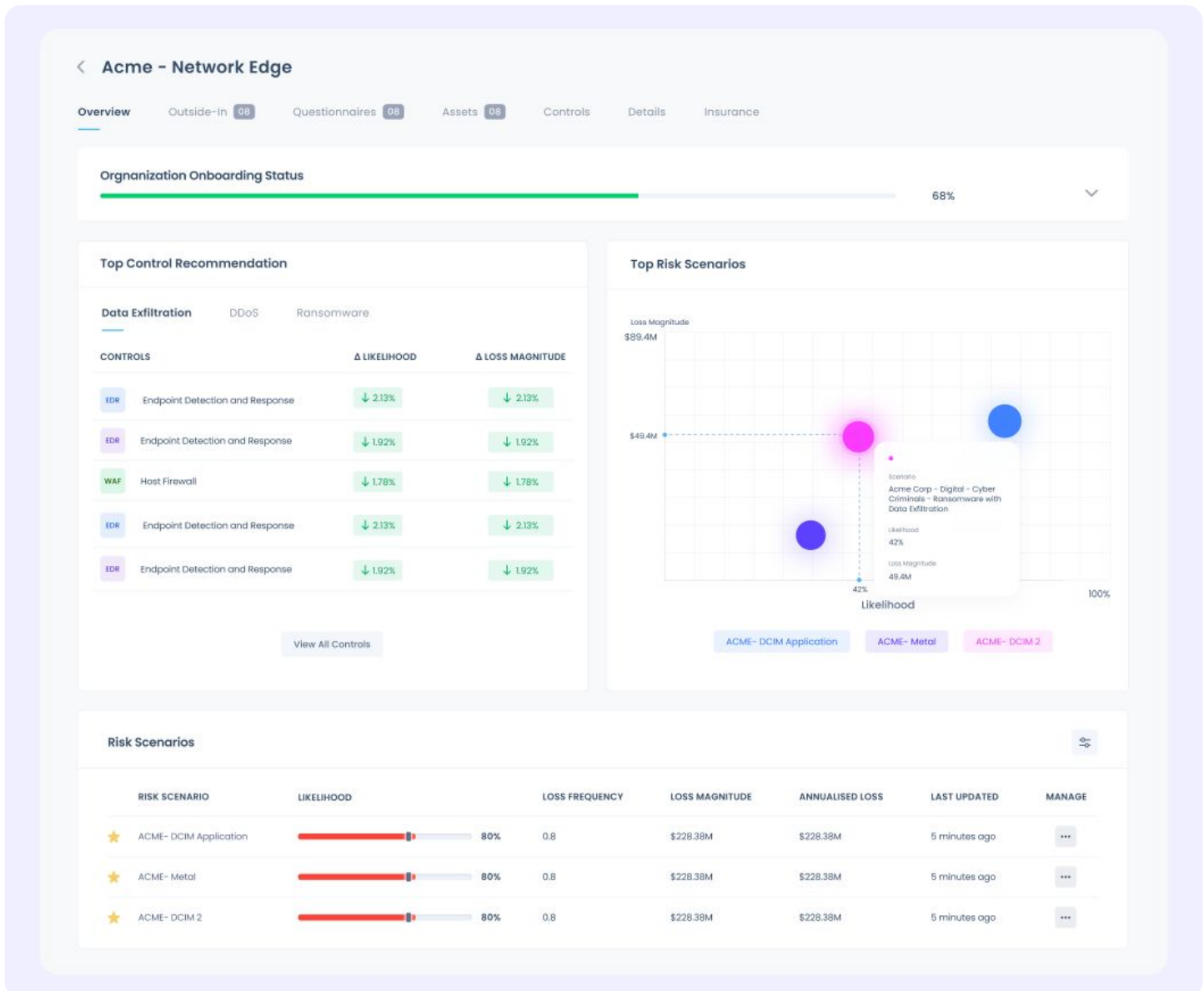


03 | Unified Third-Party Cyber Risk Management Platform

SAFE One is the only solution that enables businesses to manage their third-party and first-party risks from a single platform. SAFE TPRM continuously consolidates third-party risk data using 100% automated controls telemetry from outside-in, questionnaires, and inside-out assessments. By automatically integrating these diverse data sources, SAFE TPRM ensures that no aspect of cyber risk is overlooked.

The platform also enhances this data with context-specific threat intelligence, providing businesses with a nuanced and detailed view of potential vulnerabilities and threats. This method allows SAFE TPRM to deliver a complete, up-to-date picture of cyber risks, positioning it as the definitive source of truth for all third-party risk management needs.

The integration capabilities of SAFE TPRM extend beyond typical third-party assessments to include first-party risk evaluations, thereby offering a holistic view of all cyber risks facing the organization. This comprehensive approach streamlines the risk management process and ensures that every decision is informed by a complete understanding of both internal and external risk factors.





04 | Zero Trust-Driven Insights on Organizational Controls

SAFE TPRM incorporates zero trust principles to deliver real-time insights into organizational controls, providing a clear view of how effectively first-party controls are safeguarding against potential third-party breaches. By embracing a zero-trust model, SAFE TPRM ensures that no internal or external entity is trusted by default, enhancing security measures across the board.

The solution includes real-time scans of native controls, ensuring continuous monitoring and immediate detection of potential vulnerabilities that could be exploited through third-party interactions. This capability allows CISOs and TPRM leaders to identify weaknesses and test the effectiveness of current security controls against potential threats, maintaining a robust defense posture at all times.

Moreover, the insights generated by SAFE TPRM's zero-trust-driven data enable efficient resource allocation and informed decision-making. By understanding the strengths and gaps in your current control setup, your organization can allocate resources more strategically, focusing efforts where they are needed most to fortify defenses and minimize risks. This proactive approach ensures that your cybersecurity investments are effective and economical, supporting a secure, resilient organizational infrastructure.

Top Control Recommendations				25 of 25 Controls Assessed
NAME	PARAMETER	MATURITY PROGRESSION	LIKELIHOOD REDUCTION	
UAC	User Access Control	M2 → M3	↓ 9.31%	
HAOS	Hardened Operating System and Services	M2 → M3	↓ 8.80%	
SSW	Secured Software	M2 → M3	↓ 8.79%	
HAC	Hardened Cloud	M2 → M3	↓ 8.74%	
MFA	Multi-factor Authentication	M2 → M3	↓ 8.52%	
NFW	Network Firewall	M2 → M3	↓ 8.51%	
EDR	Endpoint Detection and Response	M2 → M3	↓ 7.90%	
UAC	User Access Control	M2 → M3	↓ 7.83%	
HAOS	Hardened Operating System and Services	M2 → M3	↓ 7.41%	
SSW	Secured Software	M2 → M3	↓ 7.32%	

[View All Control Recommendations](#)

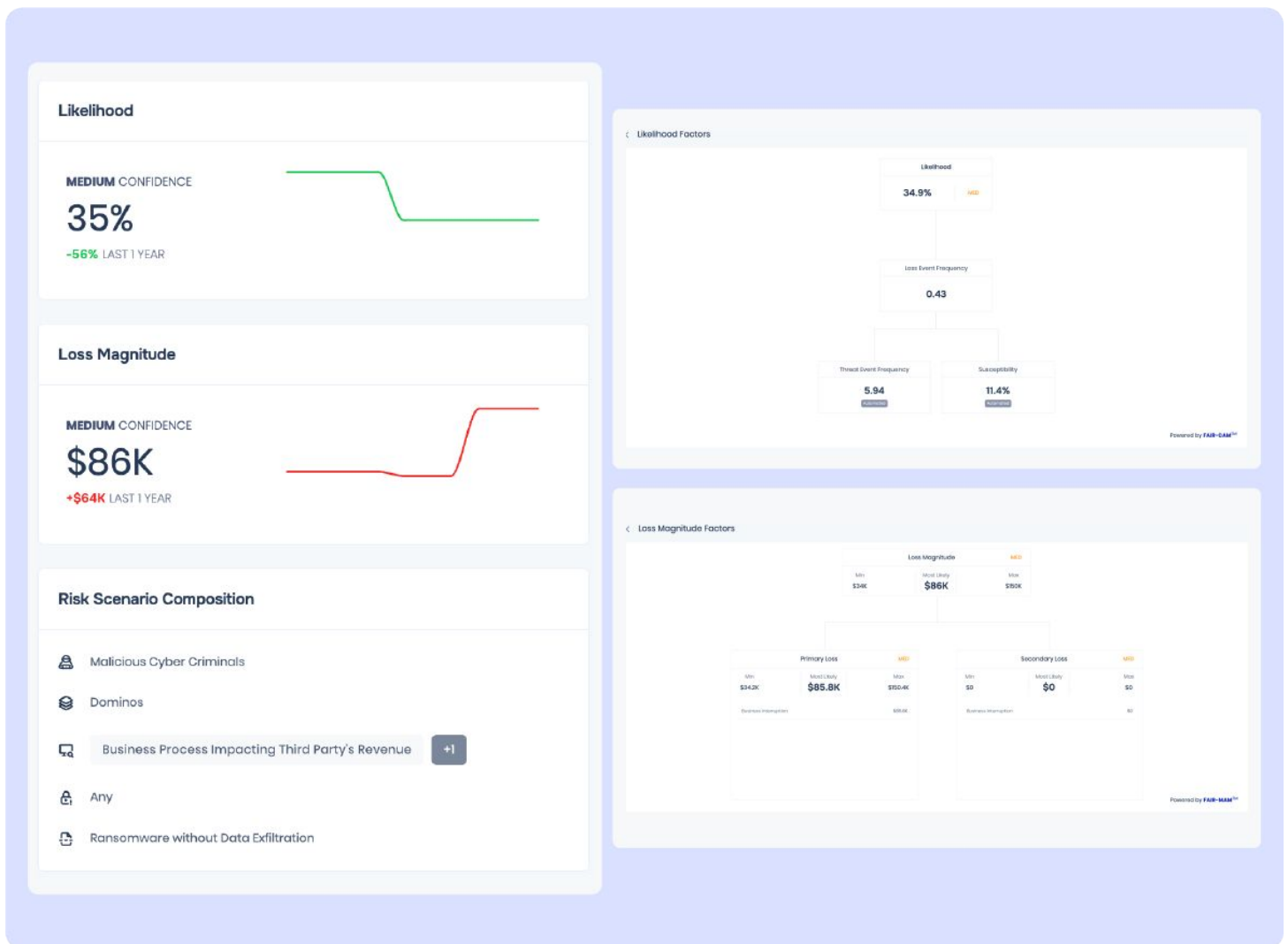


05 | Purpose-Built on Proven, Industry-Leading, Open Standards

SAFE TPRM is the industry’s most transparent and defensible solution. It sets a high standard in third-party risk management by being meticulously developed from the ground up using the FAIR™ (Factor Analysis of Information Risk) standards, including FAIR™, FAIR™-TAM, FAIR™-CAM, and FAIR™-MAM. These are internationally recognized frameworks that specialize in quantifying and managing cyber risk in financial terms, providing a solid foundation for risk assessment and decision-making.

Furthermore, SAFE TPRM enhances its robust risk management capabilities by integrating risk data with the MITRE™ ATT&CK and D3FEND frameworks. This integration provides comprehensive visibility into both third-party and first-party risks, mapping them against known attack techniques and defensive tactics for real-time threat analysis. This approach ensures that all risk management practices are aligned with global standards and guarantees that they are adaptable to the evolving nature of cyber threats.

By committing to these open and established standards, SAFE TPRM offers a transparent and defensible platform that CISOs and cybersecurity leaders can rely on for precise risk management.





06 | Reduce and Optimize the Total Cost of TPRM

SAFE TPRM introduces a cost-effective approach to managing third-party risks through its predictable and all-inclusive pricing model. Unlike traditional TPRM solutions that may charge per vendor or transaction, SAFE TPRM offers unlimited coverage of vendors without additional fees. This pricing strategy not only simplifies budget planning but also eliminates the financial unpredictability often associated with expanding third-party ecosystems.

By consolidating various TPRM tools into a single platform, SAFE TPRM also reduces the need for multiple software solutions, which can lead to significant cost savings. This consolidation enables organizations to streamline their TPRM processes, reducing both the complexity and the expense of maintaining separate systems. Businesses can manage all their third-party risks through one interface, enhancing efficiency and reducing operational costs.

Endpoint Detection and Response

Loss Event Control

EDR

Endpoint Detection and Response is a critical security control that helps...
Show More

ATTACK SURFACE

- Cloud
- Others
- Server
- Endpoint

Control Parameters

Edit

M2	M2	M3	→	51%
Capability Manual 14 days ago, Ramchandra Reddy Vemula	Coverage Manual 14 days ago, Ramchandra Reddy Vemula	Reliability Automated 16 hours ago, System		Control Maturity

Linked Controls

Search

NAME	FUNCTIONAL DOMAINS	CONTROL MATURITY	CAPABILITY MATURITY	COVERAGE MATURITY	RELIABILITY MATURITY
No records found					

Learn more about Control Maturity

Risk Scenarios

SCENARIO NAME	LIKELIHOOD	LOSS MAGNITUDE
---------------	------------	----------------

SAFE Helps You With Key Third-party Questions

<p>✔ Who are your riskiest third parties in \$ terms?</p> <p>Risk-based Third-Party Tiering: Focus on crucial vendors with tiering based on potential loss from their data access, network use, and any related business disruptions.</p>	<p>✔ How can I look at all telemetry from threat feeds and third parties?</p> <p>Comprehensive TPRM Approach: Integrates and consolidates threat feeds, and performs outside-in, questionnaire-based, and inside-out assessments for thorough third-party cyber risk analysis.</p>
<p>✔ How about my own security controls?</p> <p>Zero-Trust TPRM: Offers real-time insights into the effectiveness of first-party controls to minimize the impact of third-party breaches.</p>	<p>✔ What can I do? What can my third parties do to mitigate risk?</p> <p>Prioritized, Actionable Insights: Provides prioritized, ROI-focused recommendations to mitigate financial risks posed by critical vendors.</p>
<p>✔ How can I automate this program?</p> <p>Gen-AI-Powered Automation for TPRM: Automates data collection and security analysis to reduce manual workload and increase precision and speed.</p>	<p>✔ How can I look at all risks together?</p> <p>Simple, One-Platform Solution: Manages both third-party and first-party risks on a unified platform for holistic risk oversight.</p>
<p>✔ Is it defensible and tunable?</p> <p>Open Standards and Defensible: Leverages open standards, including FAIR, FAIR-TAM, FAIR-CAM, FAIR-MAM, MITRE ATT&CK, MITRE D3FEND, and NIST CSF.</p>	<p>✔ How can I manage my costs?</p> <p>Flat Pricing Model: Features predictable, inclusive pricing that covers unlimited vendors, helping control costs effectively.</p>



RESEARCH SPONSOR

MITRE ATT&CK, TOP CONTRIBUTOR



PUBLISHER'S CHOICE AWARD
RISK MANAGEMENT

GLOBAL INFOSEC AWARDS - RSAC 2023



BEST NEXT GEN
CYBER INSURANCE PLATFORM

GLOBAL INFOSEC AWARDS - RSAC 2023



BEST RISK
MANAGEMENT SOLUTION

CISO CHOICE AWARDS 2022™