Complete AI-Powered Third-Party Risk Management for Enterprises

Third-party ecosystems are expanding—and so are the risks. Compliance checklists alone won't cut it. You need proactive, AI-driven oversight to stay ahead.

ComplyScore®: Built for Modern Business Needs

100+ Clients	**7000** Users	**65** Countries
100+ SMEs	**100k+** Assessments	**19** Risk domains

- Unified platform for third-party risk, compliance, and governance
- AI-powered, scalable, and designed for enterprise-grade control
- Designed to replace fragmented Excel-based processes

360° Risk Management and Continuous Compliance Monitoring

- Complete visibility across your third-party ecosystem via configurable dashboards
- AI-powered scoring and automation reduce manual effort and strengthen defense
- Continuous, frictionless risk assessments with no compliance gaps
- Real-time threat and compliance insights for faster, expert-driven decisions
- Standardized workflows, scoring, and governance for smarter risk management
- Centralized data and ongoing monitoring for always-on compliance

See ComplyScore® in Action

https://www.atlassystems.com

sales@atlassystems.com

Request a demo

BITSIGHT DATASHEET

SECURING THE DIGITAL SUPPLY CHAIN

Third-Party Risk Management

Mitigate risk. Enable the business. Reduce exposure.

Overcoming New Challenges

Waves of change are disrupting cybersecurity stability and increasing cyber risk uncertainty. But CISOs and risk leaders have an opportunity to navigate that uncertainty with confidence. To manage and mitigate cyber risk from third parties effectively and efficiently. To assess and onboard new vendors while managing changing risk throughout the entirety of the relationship. And to identify and respond to critical exposure and major security events in the ecosystem.

Manage Third-Party Risk End-to-End

Bitsight TPRM is an end-to-end solution that allows CISOs and risk leaders to excel in their third-party risk programs. Risk leaders turn to Bitsight to efficiently assess and onboard vendors who match their risk tolerance, mitigate risk throughout the vendor lifecycle, accelerate outreach to third parties during majority security events, and scale the team's capacity with managed services. Bitsight TPRM serves the entire vendor relationship.

Key Benefits

- Assess new and existing vendor risk
- Continuously monitor third and fourth parties
- Effectively respond to major security events
- Scale team capacity to match business needs

"Bitsight opens conversations with our vendors' security teams. By informing them about risks they may not know about, we set ourselves up for successful business relationships from the get-go."

Ambrose Neville

Head of Information Security at the University of Surrey

Risk

Onboard and assess third-party vendors to empower business growth.

Performance

Gain visibility into your vendor network to improve ecosystem security posture.

Exposure

Prioritize, initiate, and track vendor outreach during major security events.

Vendor Risk Management

Accelerate onboarding and assessment processes to enable company growth. With Bitsight Vendor Risk Management (VRM), cyber risk leaders expedite assessments more efficiently with automated workflows, verifiable data, and a growing vendor network. Reduce vendor risk with more confidence.

Continuous Monitoring

Address ongoing risk in the digital ecosystem through the life of third-party relationships. Bitsight Continuous Monitoring empowers organizations to manage and surface ongoing risk through continuous visibility into vendor security controls, comprehensive alerting for quicker mitigation efforts, and automatic discovery of fourth-party concentrated risk. Take action as risk arises.

Exposure Management

Respond to zero-day events with speed and precision. Bitsight Vulnerability Detection & Response enables risk leaders to prioritize, initiate, and track vendor exposure. Leverage scalable templated questionnaires, tailored exposure evidence, and traceable reporting to reduce risk during critical moments.

Managed Services

Resource-constrained? Need help getting a TPRM program up and running, or improving it? Bitsight Advisory Services provides a managed service across third-party programs to manage assessments, conduct vendor outreach, support remediation plans, and improve cyber risk operations without disrupting the business.

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT

BLACK KITE

The Black Kite Difference

The Clear Advantage in Third-Party Cyber Risk Management

Black Kite is driving innovation in third-party risk management (TPRM) with a cyber ecosystem risk intelligence platform built on Accuracy, Speed, Transparency, and Collaboration. Our innovations empower organizations to make informed decisions, respond to risks with agility, and build a more resilient cyber supply chain.

Accuracy

The trusted source for defensible cyber risk data.

- Black Kite has eliminated false positives down to less than 5%, ensuring confidence when approaching vendors.
- Risk insights are delivered via a clear, intuitive dashboard.
- Vulnerabilities are shown at the asset level.

Transparency

The only open standards third-party cyber risk platform.

INDUSTRY-RECOGNIZED METHODOLOGIES

- MITRE
- CWSS & ATT&CK Frameworks
- Cyber Threat Susceptibility Assessment (CTSA) & CWRAF™
- NIST Standards (NIST 800-53, CSF, CSF v2.0.)

COMPREHENSIVE INTELLIGENCE

- Technical Ratings: Over 290+ controls mapped to 20 technical categories.
- Compliance Correlation: Supports 17 global standards with AI-driven gap analysis using UniQuE™ Parser.
- CRQ: Calculates the probable financial impact of a cyber breach to your organization using Open FAIR™.

Collaboration

The first solution that allows you to invite your vendors into the platform.

- Rapid communications on critical exposures
- Free vendor access with remediation tracking

Speed

Scale risk response with unparalleled speed.

Black Kite's continuously updated global database provides unmatched coverage and depth.

UNMATCHED DATA COVERAGE

- **500M** Domain names
- **6B** Subdomains
- **4B** Service fingerprints
- **10B** SSL certificates
- **100B** DNS and Whois records
- **100B** Web pages
- **34M+** Companies

CONSUMABLE RESULTS IN MINUTES

Dashboards:

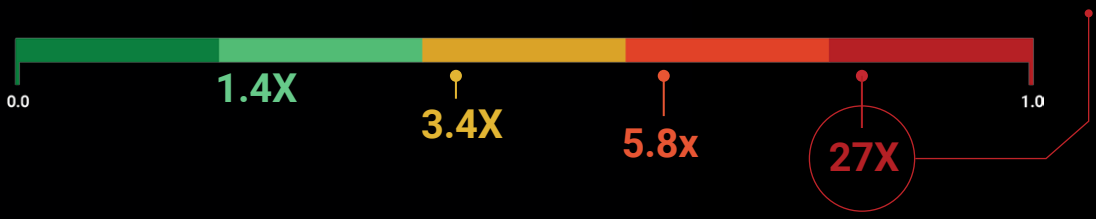
- MITRE-based letter grade cyber ratings
- Automated compliance mapping
- Cyber Risk Quantification (CRQ)
- Remediation details
- FocusTags™ threat intelligence
- Ransomware Susceptibility Index® (RSI™)

"It's the only vendor in this evaluation whose customers were unanimously satisfied with its rating accuracy.... Black Kite's unique focus on standards-based ratings tackles the industry's ratings integrity problem head-on." *The Forrester Wave™: Cybersecurity Risk Ratings Platforms, Q2 2024*

Standout Features

Ransomware Susceptibility Index® (RSI™)

The world's only tool that specifically measures an organization's likelihood of experiencing an attack by analyzing 30 controls associated with ransomware attack vectors.



In the 0.8-1.0 range, you are **27x more likely** to experience a ransomware attack than companies with an RSI value below 0.2.

FocusTags™

Real-time threat intelligence powered by Black Kite's research team identifies potential exposure to event-driven risks within your vendor ecosystem and prioritizes risks across three dimensions:

- Criticality (CVSS/CWSS)
- Exploitability (EPSS)
- Confidence levels (medium, high, very high)

Integrations

Open API and pre-built integrations with tools you use every day ensure streamlined workflows:

servicenow · coupa · Onspring · zapier · ARCHER · onetrust · LOGICGATE · SUPPLY WISDOM · ARAVO · MITRATECH · venminder

Plus: ZenGRC, Adaptive Shield, Obsidian Security, Valence Security, Rootshell Security, Balbix, BlinkOps, Templar Shield, Webhook, Standard Fusion, Revial Data Security, Navex, C1risk, and more coming.

Expertise

Black Kite's team brings unmatched knowledge and experience to our customers' success, guiding organizations of any maturity to the next level of cyber resilience.

Customer Satisfaction

Trusted by more than 3,000 customers across banking, insurance, healthcare, manufacturing, retail, and government. Consistently highly rated in customer satisfaction with a Net Promoter Score (NPS) of 75+.

Gartner Peer Insights Customers' Choice 2023 · CISO CHOICE AWARDS 2023 Visionary Company · CISO CHOICE AWARDS 2023 Third-Party Risk Management Company · Gartner Peer Insights Customer First · reddot winner 2024

Visualize Your Supply Chain

To learn more, **schedule a meeting** with us.

Coverbase

Your Vendor Management Copilot.

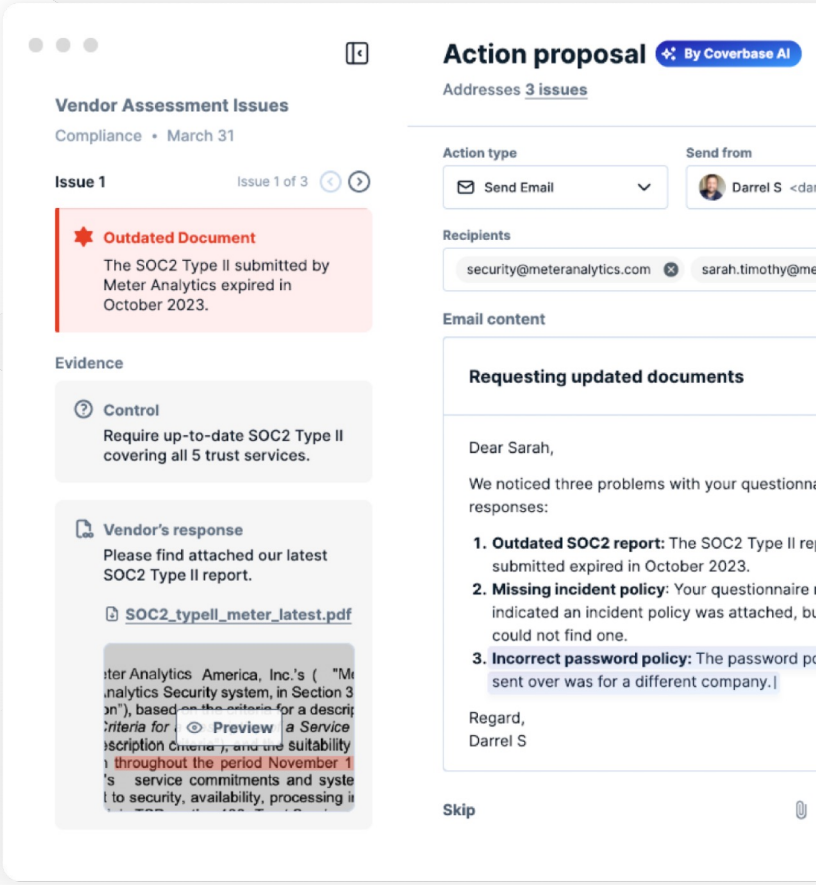
Performing security / compliance assessments on third-party vendors is highly manual and time consuming.

▶ **PROBLEM**

Manual assessments,
Time-consuming data collection,
Limited risk visibility

▶ **SOLUTION**

Automates 90% of assessments,
Frees teams to focus on mitigation,
Fast, accurate risk insights



87.6% time saved on assessments

>240 sites crawled for risk signals

10k+ vendors in peer network

Companies trust Coverbase with vendor management.

FIRST BANK · coinbase · rubrik · okta · Nationwide · bill

How it works

▶ **01**
AI gathers vendor intel
Leverage our vendor network. AI-driven email requests. Auto-fetch documents.

▶ **02**
Assessments run autonomously
Auto-assess uploads. AI analysis, evidence, recommendations.

▶ **03**
Vendors monitored continuously
Checks across security, legal, financial and operational. Alerts on updates.

For more information, **reach out to contact@coverbase.ai**

findings.

Help your board members sleep better

Your Vendor Cloud Audit is Broken.

If your VRM includes any of the following, it's not enough:

Surface-level risk scans that leave blind spots in vendor cloud environments.

Manual or so-called automated assessments are complicated, take months, and drain resources.

Constant regulatory demands, such as DORA, ISO 27001, SOC 2, and more...

A vendor risk dashboard that isn't real-time, delayed, & lacks continuous updates.

Excessive spending on VRM solutions with minimal results.

Buy back your time and effort, and let your board members sleep better so you can too.

Findings CloudVRM will easily help you to:

See the Full Picture Instantly – Real-time, continuous visibility. Stay audit-ready with insights prioritized by real engagement and risk.

Cut Assessment Time From Months to Minutes – Less back-and-forth and faster vendor approvals.

Stay Ahead, Always – Continuous monitoring detects risks before they escalate, and mitigation is automatically documented — no need to report it manually.

Save 90% on Audits – Eliminate expensive, manual third-party audits.

Easy to Use & Integrate – Integrate directly into your vendors' AWS, Azure, and GCP environments.

How we do it? – CloudVRM securely connects via API to fetch real-time security data, scans ~300 controls, & delivers a detailed report with a prioritization plan.*

Vendor Risk Management, Finally Fixed.

See how CloudVRM makes your vendors' audits easy, private and stress-free.

Book a demo today →

*Your vendor can opt-out at any moment, and the data is end-to-end encrypted

Locktivity

A better way to manage third-party risk.

Third-party risk meets business resiliency

Locktivity aligns your third party risk program with business objectives and sets risk assessments on auto-pilot.

Know your inventory

Locktivity's light touch integration identifies potential new vendors as users sign up.

Automated contextualized risk assessments

RiskFlow 360 starts with your businesses priorities and uses contextual information and automation to execute full-cycle risk management in a scalable and impactful way. Cut the busy work and focus on what matters.

Continuous visibility

Incident impact assessment? Data subject access request? Audit time? Know where your dependencies lie and where your data lives when it matters most.

Ensure compliance

Locktivity provides an out-of-the-box compliant and powerful third-party risk program, with continuous monitoring throughout the vendor lifecycle.

Trust Center

Build trust with your customers with a tailored trust page. Keep customers up to date with notifications. Access controlled and auditable.

Built by Practitioners for Practitioners

- ✓ Inherent Risk Scoring
- ✓ Pre-populated profiles
- ✓ Automated vendor discovery
- ✓ Intelligent risk assessments
- ✓ Smart automations
- ✓ Continuous monitoring
- ✓ Breach alerts
- ✓ SCIM
- ✓ SSO
- ✓ Jira integration
- ✓ Full lifecycle management
- ✓ Offboarding workflows
- ✓ Business impact analysis
- ✓ Data mapping

https://locktivity.com • info@locktivity.com • 415.234.0245

THIRD-PARTY RISK MANAGEMENT

The Last TPRM Platform You Will Ever Need

Modernize Your Program, Eliminate Trade-offs, Elevate Team Performance and Close Your Vulnerability Gap

Gain Complete Risk Visibility & Answer the Most Critical TPRM Questions

As third-party risks expand while resources remain limited, a vulnerability gap emerges from the lack of visibility and control in TPRM programs, exposing businesses to greater risks. ProcessUnity closes this gap through a best-in-class, configurable workflow platform that empowers teams to transform TPRM through four critical pillars:

TPRM Automation

Automate everything from assessment scoping to evidence collection to meaningful reports using out-of-the-box programs set up within minutes, or build a unique, configurable workflow with the help of our team.

Universal Data Core

No matter what risk domain is most important to you (financial, security, ESG, or more), we have pre-built universal data sources, including APIs, to enrich your workflow with the critical data necessary for complete third-party insight.

Global Risk Exchange

Simplify your assessment demands by accessing the world's largest third-party exchange of over 15,000 cyber risk assessments already completed by 80% of the world's most popular third parties.

AI-Powered Teams

Offload monotonous, time-consuming practices by leveraging our suite of AI-powered solutions, from evaluating inherent risk, prioritizing findings, reviewing policy documents, and predicting the effectiveness of a third-party's control.

What Customers Achieve with ProcessUnity*

- 50% reduction in oversight time
- 85% reduction in onboarding cycle times
- 85% reduction in post-contract risk assessments
- 90% reduction in time spent producing reports

*GRC 20/20 Research

Shift to a Modern TPRM Program

- Tailor to Your Team:
  Begin with an out-of-the-box program or configure a unique program and scale as necessary.
- Make Data-Driven Decisions:
  Implement data connectors, APIs, or the Global Risk Exchange to make confident decisions.
- Elevate Your Program:
  Achieve more success in your program and team through AI features and automation.

Vendor Onboarding

To confidently onboard a vendor to your business, you need to understand their risk – but not all vendors merit the same level of assessment. ProcessUnity helps you determine vendor criticality and confidentiality risk levels with inherent risk scoring to ensure vendors receive sufficient vetting at every level.

Use Case Benefits

- Reduce Onboarding Cycle Times: Eliminate delays in the time it takes to answer requests, send assessments, and evaluate vendors.
- Create Targeted Assessments: Only ask questions relevant to a vendor, improving response rate and simplifying assessment analysis.

Ongoing Monitoring & Due Diligence

Create an objective post-contract monitoring cadence leveraging ProcessUnity's powerful assessment engine. Customize questionnaire templates, establish an assessment schedule and automatically identify responses that require further review.

Use Case Benefits

- Get Relevant Data Points: Create targeted questionnaires that lead to precise information about vendor risk.
- Keep Assessments on Schedule: Implement a regular cadence for reassessment based on vendor criticality.

ProcessUnity Third-Party Risk Management significantly reduces third-party onboarding and due diligence cycle times. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest third-party risk exchange database and powerful artificial intelligence capabilities, ProcessUnity enables organizations to proactively mitigate first- and third-party risks.

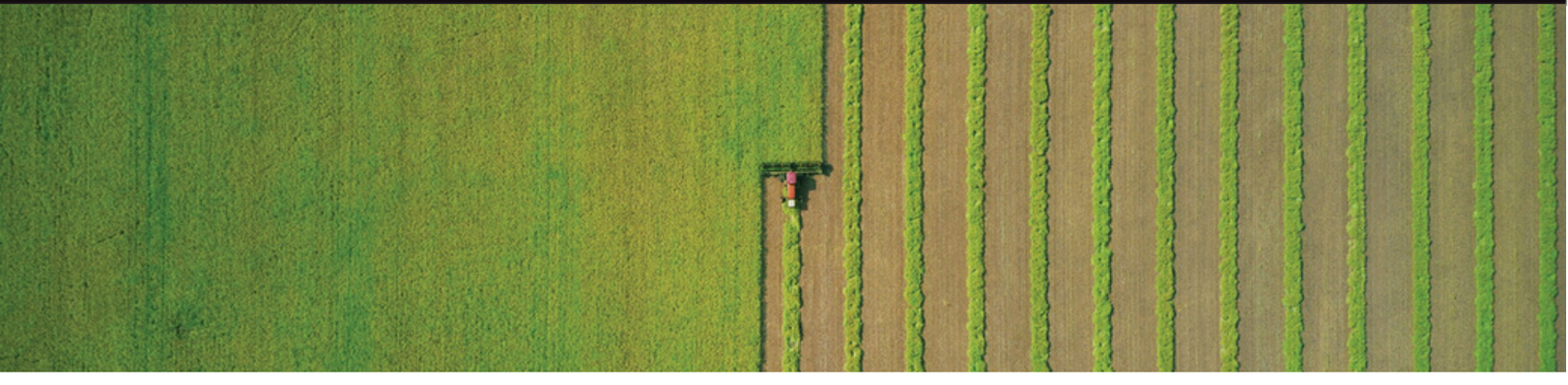
ProcessUnity

KY3P®

S&P Global

Optimise your third-party risk management approach

Businesses need to harness data, leverage technology, and deploy expertise to manage an increasingly complex supply chain risk landscape.



Stakeholders, shareholders, and regulators are increasingly explicit about their expectations of decision-makers to be equipped with accurate and timely information about their supply chain risk. Businesses must seize the opportunity within their supply network whilst managing the risk from this extended enterprise. Dynamic management is required across a wide range of risk domains:

- **Operational resilience**
- **Continuity and recovery**
- **Cyber security**
- **Geo-political**
- **Data management**
- **Legal & regulatory compliance**
- **Operational maturity**
- **ESG**

S&P Global KY3P® has a unique combination of best-in-class data, award-winning end-to-end technology, and third-party risk management expertise to provide customers with the insight to anticipate and manage the ever-changing third-party risk landscape.

At KY3P, we help your business gain valuable knowledge to navigate third-party risk and build better supplier relationships.

To learn more, visit us at:
www.spglobal .com/KY3P

or contact us:

The Americas
+1-877-863-1306

EMEA
+44-20-7176-1234

Asia-Pacific
+852-2533-3565

SAFE ONE – TPRM

Automate, Unify and Run Your TPRM Program at Scale

As the third-party attack surface explodes, these challenges overwhelm CISOs and TPRM leaders:

- **Visibility**: The conventional piecemeal approach makes it difficult to identify the riskiest vendors, making third-party risk a blind spot.
- **Mitigation**: Leaders don't have an ROI-driven, prioritized and actionable insights to quantifiably reduce third-party risks.
- **Automation & Scale**: Automating and scaling TPMR programs is challenging as it is predominantly manual with multiple siloed TPRM tools.

TPRM needs to be reimagined with an unified, automated, scalable, and defensible approach.

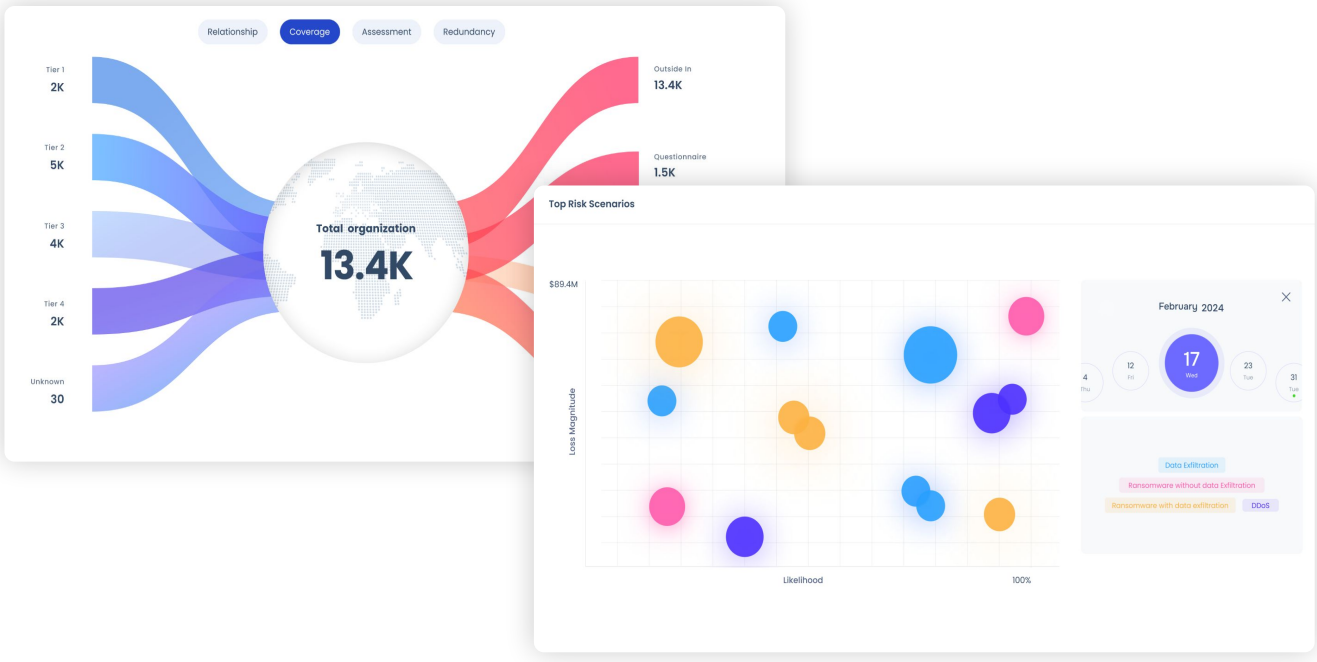
SAFE Transforms the TPRM Game

SAFE TPRM is the industry's only AI-powered third-party risk management solution, which equips businesses with the benefits of outside-in security ratings, questionnaire-based assessments, zero-trust, and inside-out scans.

Using SAFE One's unified platform, enterprises can finally get holistic, realistic, dynamic, and dollar-driven insights into their supply chain risk posture.

Does Your Existing TPRM Solution Help You To:

- ☐ **Know who your riskiest third parties are in dollar terms?**
- ☐ **View consolidated data from threat feeds and third parties?**
- ☐ **Learn how effective your security controls are against third-party risks?**
- ☐ **Enable your third parties on how to mitigate risks?**
- ☐ **Automate and scale your third-party security program?**
- ☐ **Visualize all third-party risks on a single, unified platform?**
- ☐ **Understand, tune, and defend your TPRM outputs?**
- ☐ **Optimize and reduce your TPRM program costs?**



Build, Scale, and Automate Your TPRM

01 | Focus on top-priority requirements and verify the evidence

SAFE TPRM recommends a crisp set of elite controls for vendors based on extensive research of current and past cyber attacks. It continuously consolidates third-party risk data from outside-in, questionnaires, and inside-out assessments, and aligns the findings with external threat intel to provide a singular risk view. Together with data-driven insights, control recommendations, and a unified risk view, CISOs and third parties are in a strong position to enhance resilience.

02 | Manage Third Party Risk Impact Using Zero Trust Controls

Zero trust principles drive SAFE TPRM and provide real-time visibility to an enterprise's internal resiliency controls towards its third parties. It buckets enterprise controls into likelihood reduction and business continuity controls to enable enhanced control effectiveness in minimizing third party data breaches. These insights equip businesses to redistribute resources and improve their internal cyber risk resilience – minimizing the impact of potential breaches.

03 | Partner with Third Parties to Improve their Security Programs

SAFE TPRM makes it simple, swift, and efficient to collaborate with your supply chain using AI-assisted assessments of security controls. Vendors also get a direct SAFE One platform along with access to training and onboarding modules. This enables enterprises to get a real-time view of their vendors' security posture while enabling third parties to manage cyber risk more effectively.

04 | Prioritize Third Parties based on Risk to Your Business

SAFE TPRM assesses the dollar risk and likelihood of occurrence of cyber risk scenarios such as ransomware attacks, data breaches, DDoS, and more based on third-party 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. SAFE TPRM enables enterprises to prioritize the most impactful controls to mitigate and reduce third-party risk.

05 | Reduce cost while covering all your key third parties

Users can add an unlimited number of vendors at a fixed price since SAFE TPRM pricing is independent of the number of vendors. This scalable pricing model makes it practical and efficient to grow and manage the third party risk management program as the business expands.

Gartner Peer Insights™

"It is a must need product for today in this highly vulnerable environment outside.

★★★★★

SECURITY EXPERT
IT Services, 1B - 3B USD

Gartner Peer Insights™

"SAFE dashboard is the most effective function which provides customers with real-time visibility of the current enterprise security.

★★★★★

GLOBAL LEAD CYBER SECURITY
Manufacturing, 30B+ USD

Gartner Peer Insights™

"Extraordinary Framework with good customer support.

★★★★★

SECURITY EXPERT
Telecommunication, 1B - 3B USD

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™

SAYARI

Unified Third-Party Risk Management

Seamlessly integrating risk intelligence with configurable automation to deliver transparent, actionable insights an dstreamined risk mitigation.

Transform Your Third-Party Risk Management

Managing third-party risk is more complex than ever, yet most organizations still reply on disconnected, outdated, and inefficient processes. As regulators recognize how deeply interconnected risks are, new policies are emerging to address them in a more integrated way, compelling global corporations to do the same.

THE SAYARI + CERTA DIFFERENCE

Most Up-to-Date & Adaptive

Keep pace with evolving regulations and prevent disruptions with AI-powered workflows and continuously updated risk intelligence that automates due diligence, risk adjudication, and compliance alignment.

Unified and Comprehensive

Gain a centralized, auditable, and explainable view of organizational exposure and compliance gaps.

Scalable & Configurable

Automate risk mitigation processes with configurable and scalable workflow automation supporting multiple high-impact risk domains — including ABAC, ESG, cyber, financial, and supply chain — that adapt dynamically to organizational needs and compliance policies.

> **Sayari's trade screening solution in Certa enabled us to quickly identify critical diversion risks related to our Turkish customer set that could have significantly imperiled our operations.**

Trade Compliance Head
Fortune 100 Oil & Gas Company

TRUSTED BY THE REGULATORS AND THE REGULATED

U.S. Department of Homeland Security (DHS)

HM Revenue and Customs (HMRC)

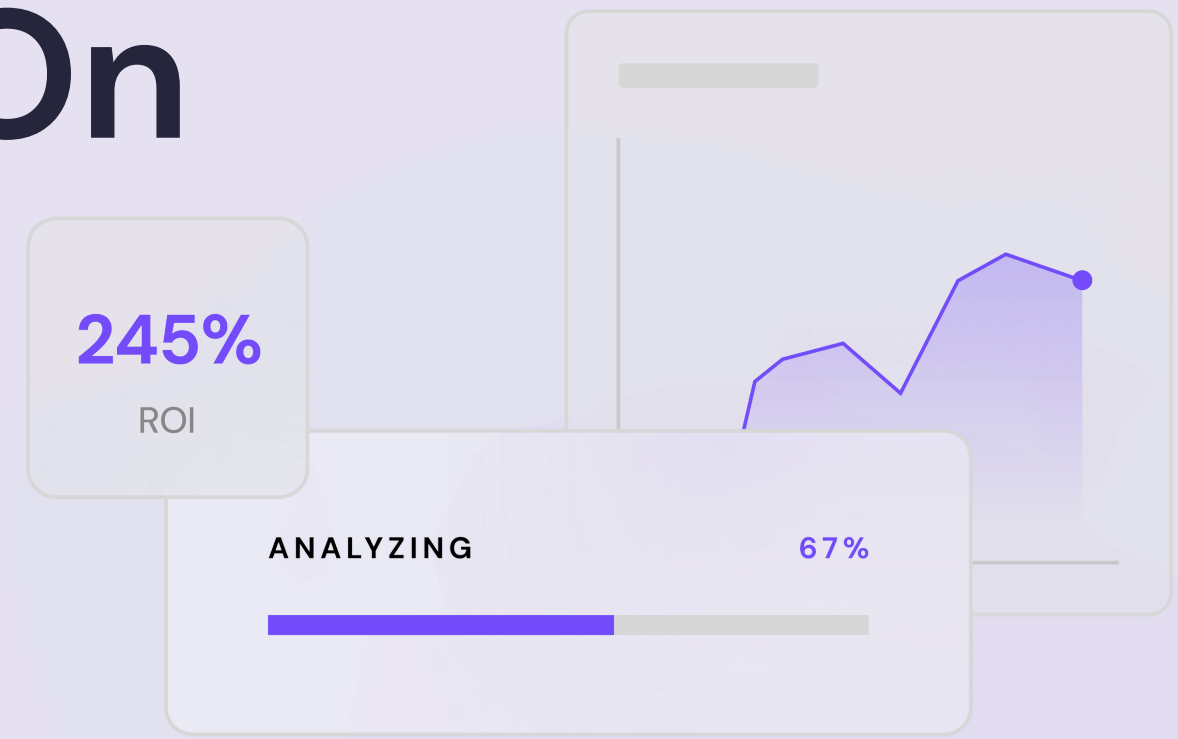
Office of Foreign Assets Control (OFAC)

Customs and Border Protection (CBP)

Visit sayari.com to request a personalized demo >

Third-Party Risk Intelligence You Can Act On

Gain real-time visibility into your extended network of vendors, partners, and customers—and detect emerging risks before they impact your operations, reputation, or compliance posture.



Continuous Monitoring of Third-Party Exposure

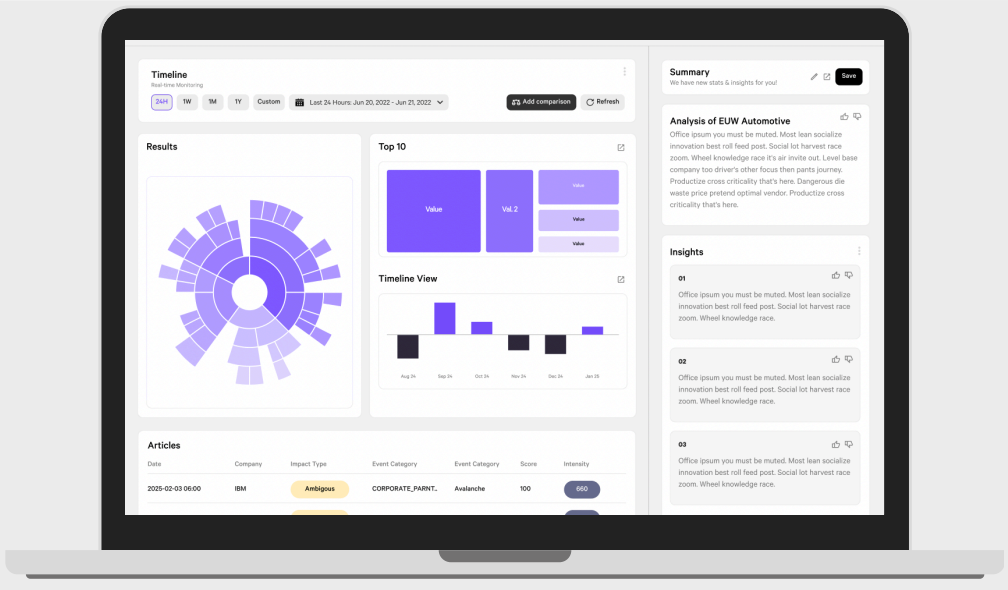
12 languages, 1.9M+ OSINT sources: scanning global media, social channels, news outlets.

Daily alerts & customizable dashboards: focus on the metrics that matter to you.

Adverse-media tracking: catch hidden signals—from data breaches to ESG controversies.

Detect Risks Beyond Contracts

From cyber breaches to regulatory violations, our AI spots hidden signals that audits miss—so you can intervene before risks escalate.



- **svEye™ multi-tier mapping**: visualize complex supplier-and-partner networks.
- Empower procurement, legal, and compliance teams with structured, **real-time insights**.
- Identify **early risk signals**—and new opportunities—in one unified view.

www.semantic-visions.com

Supply Wisdom®

Turning Risk into Resilience.

About Supply Wisdom

Supply Wisdom transforms enterprise risk management with comprehensive, predictive, real-time risk intelligence. Through continuous monitoring, comprehensive intelligence reports, and real-time alerts, Supply Wisdom prevents and mitigates enterprise risks, and unlocks revenue opportunities.

4%
Customer Revenue Growth

311%
Return on Investment

3,700+
Hours Saved on Average

SPEED = REVENUE

Continuously monitor all of your critical third parties and locations; mitigate risks in real-time. Our customers have seen up to 311% return on investment.

FIRST STEP IN GLOBAL COMMERCE

Redefining the enterprise risk function to approve new initiatives in hours, not months. Our product rapidly identifies the 98% of all third parties and locations that are safe to do business—and the 2% that are not.

COMPREHENSIVE COVERAGE

Monitor all seven risk domains. Financial, Cyber, Operations, ESG, Compliance, Nth Party are all tagged to the 7th domain, Location. Integrate with your existing systems.

IMMEDIATE DORA COMPLIANCE

Buy continuous location monitoring online and fill the largest compliance gap enterprises face with the EU Digital Operational Resilience Act (DORA).

According to Gartner, 84% of enterprises have faced a third-party vulnerability or risk event, leading to operational disruption, supply chain interruption, and regulatory action. **As geopolitical events and external partnerships become increasingly complex, businesses need advanced, automated, real-time ways of knowing any risks among their customers, partners, and downstream vendors.**

SAMPLE CUSTOMERS

UnitedHealthcare
Santander
Bank of Ireland
CDPHP
BNY MELLON

Also....

One of the three largest telecommunications providers in the world
One of the three largest social media companies in the world
One of the three largest investment brokerages in the U.S

Supply Wisdom® www.SupplyWisdom.com

Contact us today for a demo or consultation.

CYBER SUSTAINABILITY OPERATIONS FINANCIAL COMPLIANCE LOCATIONS NTH PARTY

Transforming vendor risk management from checkbox tasks to scalable insights with Vanta

Manage vendor risk at scale through a transparent, efficient, and comprehensive view of your vendor portfolio.

Vanta helps you accelerate the vendor security review process and uncovers actionable insights that enable proactive vendor risk management.

Vendor risk management is a tedious, manual task—one that's necessary for security and compliance but rarely gets the attention it deserves. With the increase in third party breaches, the proliferation of SaaS tools, and emerging AI technologies, vendor risk management is now more important than ever.

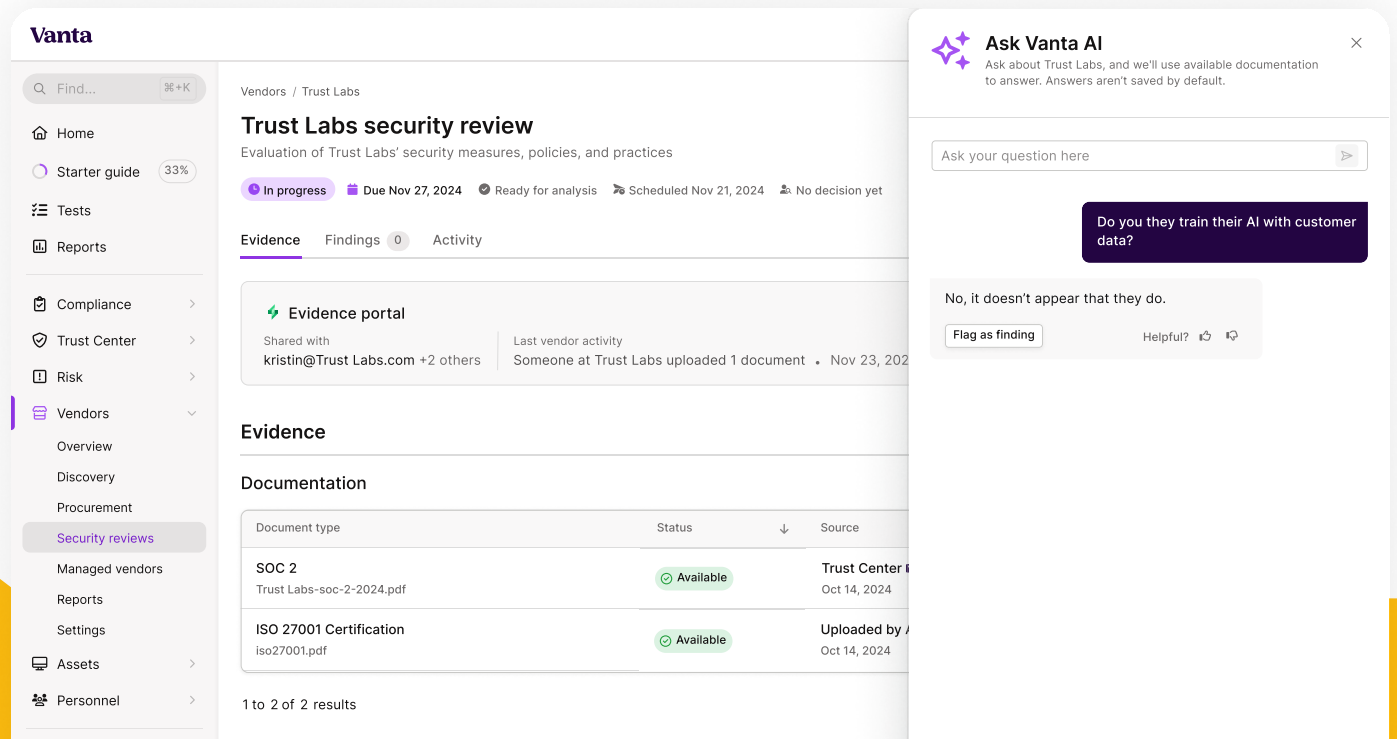
Actionable insights

At Vanta, VRM isn't just a compliance checkbox, but a strategic, value-driven part of your broader Governance, Risk, and Compliance (GRC) program. Our solution surfaces the most important and actionable vendor risk insights, helping you focus on what truly matters: identifying real risks, creating remediation plans, and tracking it all back to your risk program.

AI-powered vendor security reviews

Vendor security reviews are time consuming and overwhelming — from prioritizing the most important vendors to , collecting required evidence, processing large volumes of data and identifying emerging vulnerabilities. With Vanta, AI and automation are at the core of our security review process, improving efficiency and accelerating risk detection. Our AI-powered tools reduce the time it takes to complete a vendor security review by up to 50%! Vanta empowers your team to stay ahead of evolving security risks while minimizing manual effort. Leading to stronger security posture and faster response times, so your team can act fast on critical security findings.

> "It used to take us 50 hours per vendor to perform a security review, a process my team has to repeat across more than 50 vendors annually. Vanta's Vendor Risk Management solution allows us to reduce this to only a few hours a week for each vendor, freeing up time to focus on more strategic security objectives."
>
> George Uzzle,
> Chief Information Security Officer
>
> VIBRANT HEALTH



Integrated vendor risk

Managing vendor risk separately from your organizations risk management efforts creates gaps in your overall risk monitoring system. Vanta's VRM solution integrates seamlessly with your broader security and compliance programs, allowing you to track and monitor vendor risk within the same platform. This integrated approach feeds directly into your GRC program, enabling you to demonstrate due diligence in third-party risk management to auditors and customers.

Comprehensive view

One of the biggest challenges in vendor risk management today is tool sprawl. With fragmented systems, companies struggle to get a complete, unified view of their third-party risk resulting in isolated data, incomplete insights, and higher exposure to risk. Vanta's VRM solution provides a comprehensive, integrated space to manage all vendor risk data. Whether you're tracking vendor performance, security posture, or compliance status, our system consolidates it all, offering a real-time, holistic view of your vendor ecosystem.

Leverage automation and Vanta AI to reduce the time it takes to complete a security review by up to 50%

Vanta AI

Let Vanta AI do the tedious work for you—from answering preset questions to re-analyzing documents— saving you time and resources.

Customized risk rubric

Use Vanta's rubric to auto-assign default risk scores, or manually assign risk levels, based on your criteria.

Security templates

Use pre-built questionnaire templates or create your own—and let AI do the rest.

First party data

Access first-party data through Vanta's growing network of Trust Centers, giving you a more accurate view of your vendor risk.

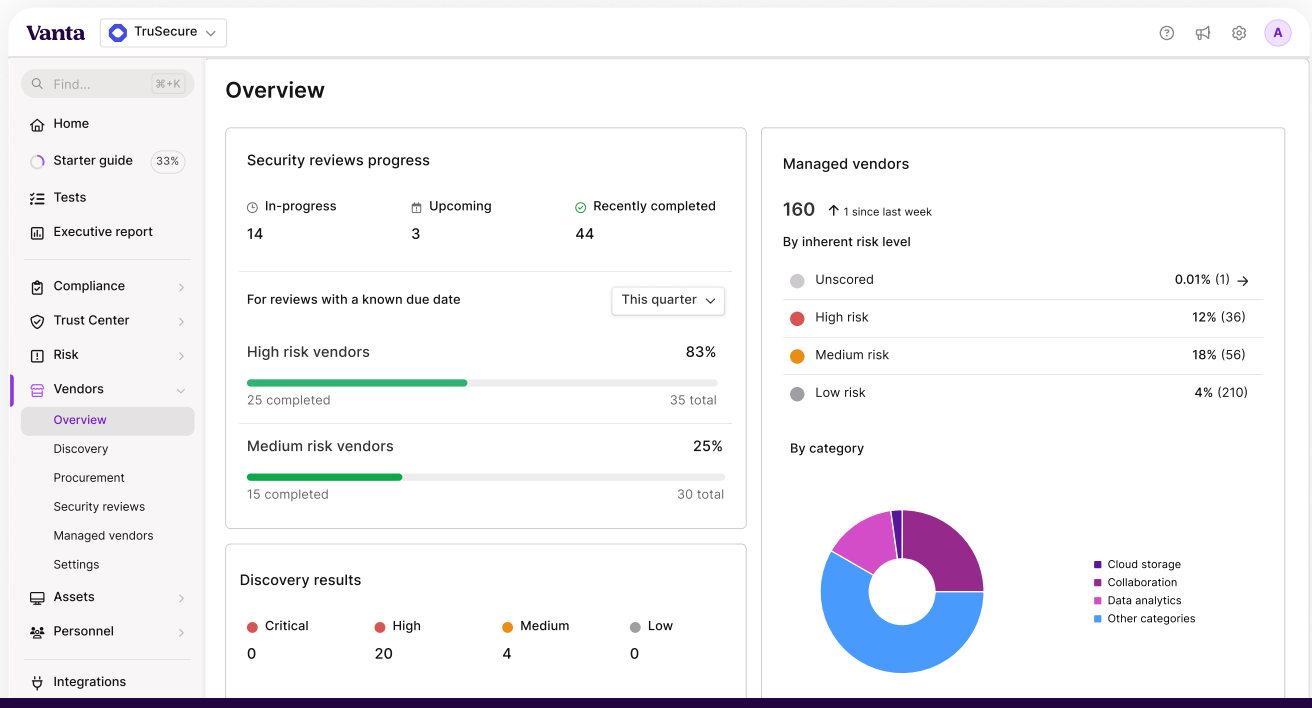
Smart vendor communication

Automatically request evidence from vendors, and book follow-ups so no details fall through the cracks.

Procurement integration

Streamline workflows and stay on top of procurement requests by connecting your procurement system with Vanta.

> "We use Vanta for VRM, which helps us immensely. The AI feature pulls out the most important details so we don't have to spend time combing vendor documentation word for word."
>
> Mandy Matthew,
> Lead Senior Security Risk Program Manager
>
> duolingo



Vanta

Automate compliance. Simplify security. Demonstrate trust.

Vanta is the leading trust management platform that helps simplify and centralize security for organizations of all sizes. 10,000+ companies, including Atlassian, Omni Hotels, Quora, and ZoomInfo, rely on Vanta to build, maintain, and demonstrate trust—all in a way that's real-time and transparent. Founded in 2018, Vanta has customers in 58 countries with offices in Dublin, London, New York, San Francisco, and Sydney.

To learn more, visit: www.vanta.com | sales@vanta.com