BITSIGHT

EBOOK

10 Pillars of a Resilient Third-Party Risk Management Program

By Chris Poulin

Table of Contents

Today's Third-Party Risk Management Challenges 3

What Does a Strong TPRM Program Look Like? 9

1. Selection (RFP/x, M&A) and Inherent Risk Assessment
2. Residual Risk Assessment
3. Contract Negotiations
4. Onboarding
5. Collaboration
6. Monitoring
7. Fast Response When Vulnerabilities Hit
8. Offboarding
9. Workflow Management
10. Metrics and Reporting

Conclusion 16

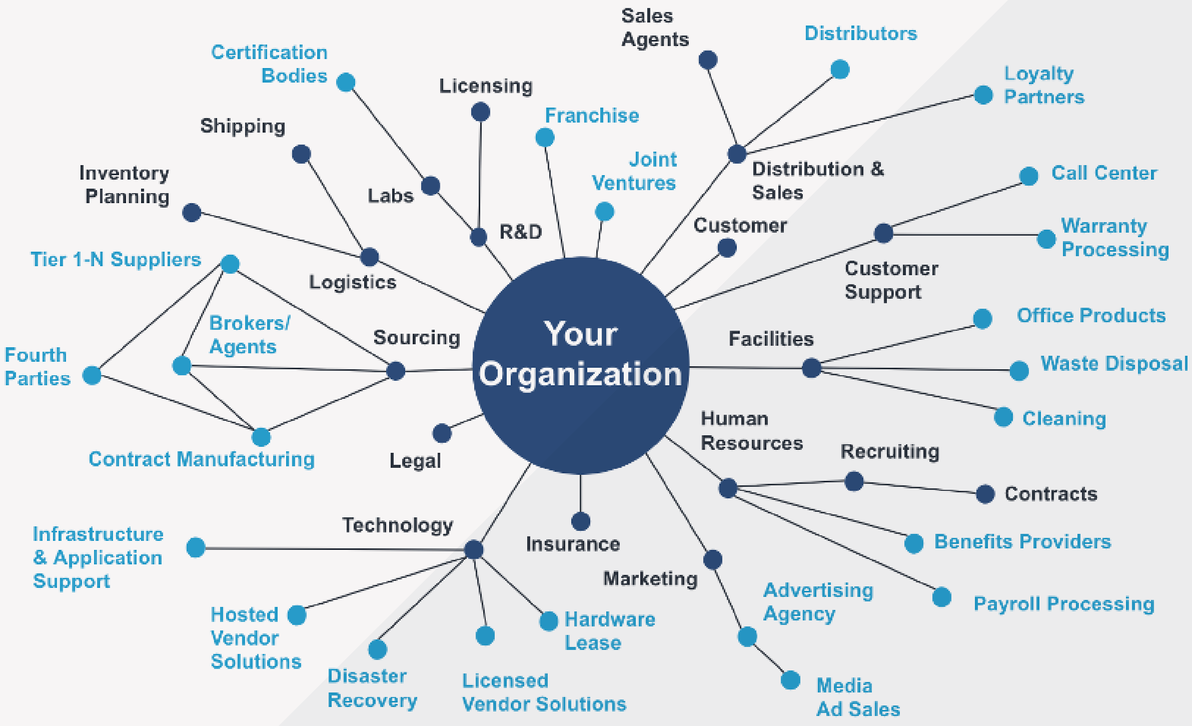
01

Today’s Third-Party Risk Management Challenges

01 Today's Third-Party Risk Management Challenges

Digital transformation is driving the expansion of organizations' digital ecosystems and their extended enterprises. Today, the majority of businesses have a moderate to high dependency on external entities, including vendors, third parties, fourth parties, and beyond. Add in the evolving regulatory landscape and necessary enforcement across jurisdictions and it becomes clear: third-party cyber risk is now a board-level compliance issue.

While the business opportunities from extending an organization's ecosystem to an external provider may be significant, outsourcing to a third party also puts the organization at risk of exposure and breach. Breaches attributed to third-party involvement have doubled from 2024,[1] and the Change Healthcare data breach in February of 2024 affected about one-third of the US population and nearly all (94%) of US hospitals that use Change Healthcare as a vendor.[2]



With the acknowledgement that relying on third parties expands an organization's attack surface, it's safe to say that third-party risk management (TPRM) no longer is an option: it is a requirement for organizations to protect their reputation, intellectual property, data, and competitive advantage. However, almost two-thirds of organizations lack confidence in their TPRM programs.[3]

Pushed by increasing cyber threats, increased regulatory and internal pressures, and the need to continue expanding digital footprints, there's a growing awareness that more due diligence is needed. Forward-thinking TPRM programs are starting to align internal practices and vendor assessments with these emerging standards, ensuring readiness, resilience, and cross-border defensibility. However, it can be overwhelming to know where to start or how to scale when it comes to managing third-party cyber risk.

Increased Regulatory Focus

GDPR | DFAR | FFIEC | NIST | Hong Kong Monetary Authority | APRA | DORA | NIS2 | U.S. Securities and Exchange Commission

[1] 2025 Data Breach Investigations Report (Verizon Business, 2025)

[2] Change Healthcare breach affected 100,000,000 patients (Medical Economics, 2024)

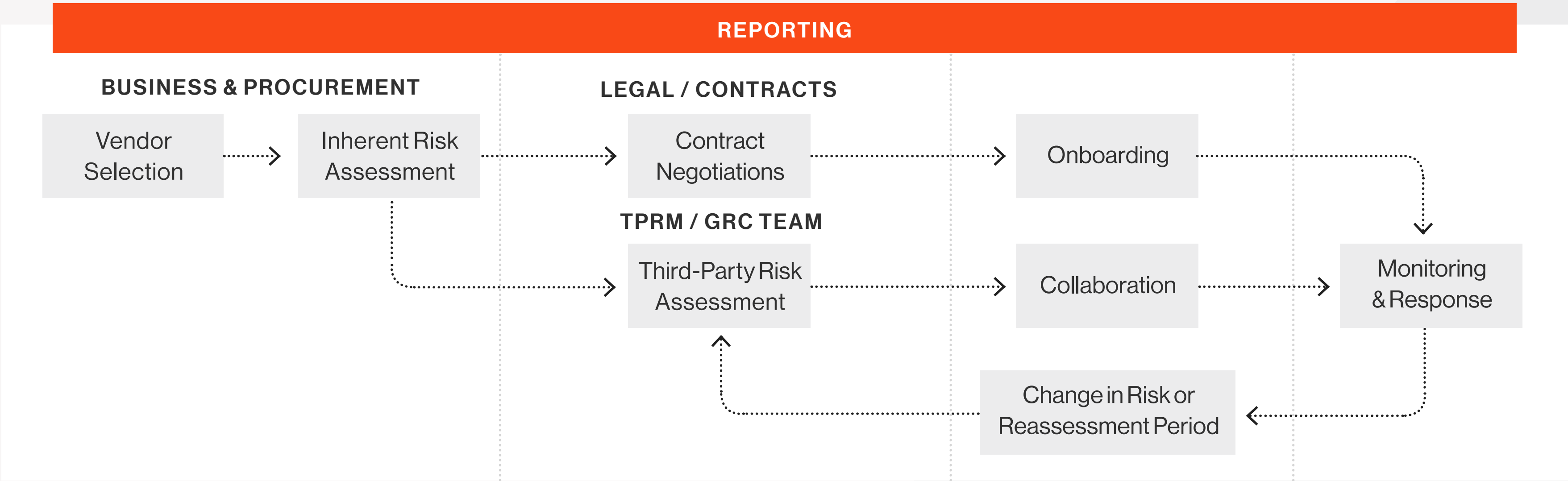
[3] How well do you know the risks posed by your third parties and supply chain? (PwC, 2022)

02

What Does a Strong TPRM Program Look Like?

02 What Does a Strong TPRM Program Look Like?

It’s useful to first understand how the majority of TPRM programs operate before discussing how to stand up and optimize one. Additionally, it’s beneficial to have a high-level understanding of where technologies can come in to assist, as seen in the model workflow. Next, we’ll dive into how each relates to the 10 pillars of a resilient TPRM program.



- Impact and Criticality
- Tiering
- Bitsight Rating
- Thresholds / Correlation Studies

- Establing Trust
- Questionnaires and Document Review
- Bitsight Rating and Risk Vectors
- Questionnaire to Data Mapping

- Vendor Outreach
- Enable Vendor Access
- Reassessment Considerations

- Supply Chain Security Incidents
- Breaches
- Ransomware
- Disruptions

01.

Selection (RFP/x, M&A) and Inherent Risk Assessment

The selection process usually begins with a Line-of-Business (LOB) buyer making a request to Procurement.

This triggers an Inherent Risk Assessment, composed of a small set of questions to determine what the risks are to the organization by doing business with the vendor. The questions typically number between 10 and 20 and cover both enterprise and cybersecurity risk. An example question panel might look like the chart on the next page.

If the answers to the Inherent Risk Questionnaire (IRQ) indicate a cybersecurity assessment is merited, then the cybersecurity team responsible for evaluating vendors (referred to from here on as Cyber Risk) will be pulled in to perform a Cyber Risk Assessment (i.e. Residual Risk Assessment).

In today's hyperconnected environment, it's increasingly rare for a third-party engagement not to warrant some level of cybersecurity assessment. But the depth of that assessment varies widely—and rightly so. Take forklifts as an example. For a global manufacturer, these aren't just warehouse equipment; they're operational assets with IP addresses that feed into centralized logistics systems. If those systems go down, the cost of downtime can run into the millions. Meanwhile, a small business with a single forklift that offloads deliveries twice a quarter has an entirely different risk profile. Inherent risk is highly contextual. The more we tailor assessments to reflect business impact, the more effective—and defensible—our TPRM programs become.

In some organizations, instead of or in addition to an inherent risk evaluation, a Risk Review Board can decide whether there's a cybersecurity component to engaging with a vendor. Including the Cyber Risk team will help identify cyber risk either before deciding to do business with a vendor (optimally) or, in the worst case, after the vendor is already engaged.

Inherent risk assessment also results in tiering vendors by criticality. A common tiering practice is to have three or four tiers, sometimes labeled Tier 1 through Tier 3 or Critical, High, Medium, and Low. These reflect the impact on your organization if the vendor suffers a breach or engages in unsafe practices that expose your data or systems to unauthorized access. The tiers will define the level of rigor and effort required to monitor the vendor and manage the relationship.

Example question panel:

RISK AREA	RISK TYPE	QUESTION
Enterprise	General	What is the nature of services or products, as well as the industry, to be provided by the vendor?
Enterprise	Continuity / Dependence	What is the financial strength / credit worthiness of the vendor?
Enterprise	Dependence	How long has the vendor been in business?
Enterprise	Continuity / Dependence	What percentage of the vendor's revenue will come from us?
Enterprise	Governance / Compliance	What oversight does the vendor have?
Enterprise	Governance / Compliance	Is there a compliance and regulatory risk associated with the vendor's service or product?
Enterprise	Reputation	Have there been complaints or lawsuits filed against the vendor?
Enterprise	Geopolitical / Continuity	What is the likelihood of fraud, corruption, political unrest, and/or natural disasters to disrupt the vendor's services or product?
Enterprise	Continuity / Dependence	What is the impact on our business operations due to an availability issue with the vendor?
Enterprise	Extended Risk	What is the extent of a vendor's outsourcing (fourth party / subcontractors) relative to our data and systems?
Cyber	Data	Which classification/sensitivity of data will the vendor have access to?
Cyber	Data / Compliance	Is the data subject to regulatory or contractual governance?
Cyber	Connectivity	How is data transmitted as part of the services provided?
Cyber	Systems / Connectivity	Will the vendor have connectivity or remote access to our network and systems?
Cyber	Data / Governance	How long will the data be retained by the vendor?

02.

Residual Risk Assessment

Residual risk is what remains after evaluating controls to mitigate the inherent risks. For example, if you outsource your patient billing to a third party, then the inherent risk is high (probably Tier 1 or Critical) since the data is governed by regulations and exposure is a reputational risk.

This is especially critical when third parties are handling regulated data or operating in regions subject to evolving laws—such as the EU's Digital Operational Resilience Act and NIS2 Directive—which are raising the bar for supply chain security, reporting obligations, and vendor oversight. But if the third party stores the data on a network segment that's separated from other business data, requires multi-factor authentication and contextual access controls, stores logs for every transaction, and alerts on anomalous behavior, then the residual risk is much lower.

Once Cyber Risk is engaged, they'll typically send a questionnaire to the vendor asking about their cybersecurity policies, processes, and procedures. The questionnaires are based on one or more standard cybersecurity frameworks, with some customization. For example, an organization may use ISO 27001 or the NIST Cybersecurity Framework (NIST for short) as the base framework and then add specific control questions from the Payment Card Industry's Data Security Standard (PCI DSS).

There are two common challenges of this step:

01.

Too many vendors to assess and limited resources at disposal.

02.

Exchanging questionnaires and artifacts as evidence can be clumsy.

To tackle the first one, many organizations are trimming down the traditional format of about 200 questions and using responses to the IRQ—as well as external data sources such as Bitsight—to pinpoint the control areas they want to review in depth, which speeds up the process without deteriorating effectiveness.

The second challenge is largely due to how these communications are traditionally operated. Relying on spreadsheets and emails can expose security practices and gaps to unauthorized parties and potential attacks. Getting a satisfactory response from vendors is rarely a one-time activity, which often results in back-and-forth transmittals and delays in the assessment process.

Cyber Risk combs through questionnaires, artifacts, ratings, and other evidence and then flags anything that doesn't align with your risk tolerance, logging gaps in a register with clear action plans and deadlines. That register becomes the foundation for decisions, including whether the business accepts the risk, chooses a better-aligned vendor, or escalates it. Occasionally, Cyber Risk has veto power—but more often, they're the signal in the noise, helping the business make informed, risk-aware choices.

Good practices that have been proven productive across industries involve:

Adoption of questionnaire portals, or online questionnaires with interactive, contextual question sets. This enables hiding or exposing groups of questions depending on the service types and responses to previous questions. It also ensures a complete questionnaire. Examples include: Enterprise and IT GRC platforms (such as ServiceNow and RSA Archer) and purpose-built vendor risk platforms such as Bitsight Vendor Risk Management (VRM).

Analyzing vendor artifacts, such as security policy and processes, infrastructure diagrams, and audit reports like SOC 2 Type 2, ISO 27001, and PCI. Cybersecurity ratings and other analytics are also considered as evidence.

Cyber Risk combs through questionnaires, artifacts, ratings, and other evidence and then flags anything that doesn't align with your risk tolerance, logging gaps in a register with clear action plans and deadlines. That register becomes the foundation for decisions, including whether the business accepts the risk, chooses a better-aligned vendor, or escalates it. Occasionally, Cyber Risk has veto power—but more often, they're the signal in the noise, helping the business make informed, risk-aware choices.

03.

Contract Negotiations

Contract review and redlines are required when preparing to onboard a vendor. This generally takes place after the inherent risk assessment and possibly after the cybersecurity assessment (or in parallel).

It's important to build language into the contract that states the vendor agrees to:

- Maintain a certain level of security rigor.
- Comply with requests to audit the vendor (Right to Audit).
- Work with you to address risks that fall below your risk tolerance threshold.
- Notify you when they have a change in their security posture or when they experience a cybersecurity incident.
- Accept sanctions based upon non-compliance with the risk standards.

04.

Onboarding

The steps to onboard a vendor are dependent on the services or goods they provide, as well as their organizational policies and procedures, among other factors. At a minimum, the following should be accomplished:

- Enter the vendor and contract terms into a vendor inventory system, usually owned by Procurement.
- Collect and register the points of contact at the vendor's organization, as well as the vendor relationship manager in your own organization. These will be critical when you need to reach out to the vendor for reassessment and to remediate existing or newly observed risks.
- Enter any outstanding risks into a risk register for remediation or mitigation.
- Train the vendor on your policies and processes.

Assessing and communicating with vendors can be time-consuming. Organizations have seen early success in using AI-enhanced tools to streamline due diligence—introducing document parsers, questionnaire analysis engines, compliance mapping functions, and workflow automation to replace the grind of spreadsheets and email threads.

But parsing vendor artifacts is only a fraction of the battle. The real opportunity lies in transforming the way teams collaborate, gather context, and make sense of risk. As large language models (LLMs) become more integrated into the TPRM workflow, we're seeing major gains not just in speed, but in the depth and continuity of analysis. AI can help correlate questionnaire responses with security ratings, identify inconsistencies across audit artifacts, and even draft remediation plans based on predefined risk thresholds.

More importantly, the combination of contextual understanding —with insights drawn from threat intelligence and objective, real-time security data—gives risk teams a clearer view of what actually matters. AI can be an accelerator for that. It's not just about checking boxes. It's about accelerating the path to risk clarity, aligning stakeholders around priorities, and knowing when to act. That's the unlock: less time chasing vendors for clarification, more time focused on the risks that could materially impact your business.

05.

Collaboration

After onboarding—and sometimes before—you'll want to work with vendors to address gaps in their cybersecurity practices that fall below your organization's risk tolerance threshold. The risk register provides the punch list of items to address and results in a remediation plan that's a collaboration between your organization and the vendor's.

While this sounds simple on the surface, it becomes complex:

- It can be difficult to identify the vendor relationship manager in your own organization and the relationship manager at the vendor's organization.
- You're working with people with agendas and emotions. They may interpret your request as a criticism of their own efforts and not a program-level gap.
- Every cybersecurity team on the planet is resource-constrained and often will push back on requests or deadlines.
- Organizations are often complex and it can be difficult for the vendor to identify who's responsible for a system or practice, particularly when they may have acquired companies that are operating independently or allow business units to operate autonomously. This can be further complicated by geography and country-specific regulations.

Nevertheless, it's important to craft a plan with timelines and consequences, including financial sanctions and contract termination. The cybersecurity team sometimes handles creating the plan in conjunction with the vendor relationship manager, but more often a separate team responsible for ongoing monitoring will manage the execution of the remediation plan.

06.

Monitoring

Traditionally, monitoring is relegated to reassessing vendors. A typical cycle is every one (1) year for critical and high (tier 1 and sometimes tier 2) vendors, and every two to three years for those that fall into lower tiers. Note that this is aspirational; many organizations don't have the resources to even reassess critical vendors every year.

Monitoring also includes keeping track of news about your vendors and when they experience a cybersecurity incident. In most contracts, the vendor is required to report changes in their security posture or cybersecurity incidents, which would also trigger some form of reassessment. This may take a few forms:

- A full assessment, including requiring the vendor to fill out a new questionnaire and providing artifacts and recent audit reports.
- A partial assessment, focusing only on critical cybersecurity practice areas.
- A recent audit report.
- A remote or onsite audit or spot-check.

As with the initial assessment, the reassessment may result in the Cyber Risk team recommending that the LOB find another vendor, sanction the vendor, or proceed with business as usual.

07.

Fast Response When Vulnerabilities Hit

When a critical CVE drops, minutes matter. With attackers moving faster and exploiting AI to scale their campaigns, third-party vulnerabilities can become your exposure—fast. While this falls under continuous monitoring, the speed and intelligence of your response now defines the effectiveness of your third-party risk program.

Start with an incident response plan (IRP).

Ensure alignment across Cybersecurity, Legal, Procurement, and key business stakeholders so the right people act quickly and confidently—based on shared risk context.

Prioritize exposure using CTI.

Go beyond vendor attestations. Combine threat intelligence with asset-level and version-specific data to pinpoint which third parties are likely affected, and which vulnerabilities are actively being exploited in the wild.

Scale outreach with context.

Equip vendors with clear, actionable data in the format of pre-built, evidence-supported questionnaires and targeted communications to help them understand the threat and move swiftly to mitigate it.

Track and adapt.

Use workflows to monitor who's been contacted, what action they've taken, and how remediation aligns to your risk thresholds. Analyze performance metrics like time-to-discovery and vendor response rates to harden your process.

Today, many organizations are still juggling vulnerability response across disconnected systems, including GRC tools, spreadsheets, and inboxes. That fragmented approach slows everything down just when speed matters most. If that sounds familiar, it's time to rethink your strategy. I have seen more and more organizations look for integrated platforms to detect, prioritize, communicate, and remediate vulnerabilities across the third-party ecosystem. Managing cyber threats in an end-to-end platform significantly helps teams to handle this in an agile, scalable way.

08.

Offboarding

An often-absent aspect of TPRM programs is the offboarding process, including monitoring the vendor after the contract has been terminated. Many contracts state that the vendor will expunge all data upon dissolution of the partnership; however, many third parties don't have the procedural triggers or the means to follow-through on the contract terms. It's in your best interest to continue to monitor vendors for a period of time after the contract is terminated to ensure they don't suffer an incident that exposes your protected information.

More advanced programs are pushing this further—partnering with providers who can detect unknown assets attempting to connect to their networks, and using telemetry to attribute those assets. This makes it possible to flag instances where offboarded vendors still retain access they shouldn't. It's a smart way to turn passive risk into actionable intelligence and close the loop on your vendor lifecycle.

09.

Collaboration

As mentioned earlier, many organizations manage vendor assessments and vendor inventories using spreadsheets and other general-purpose tools. However, the workflow is complex and requires a number of groups that don't share the same management structure to participate:

- Procurement may use a vendor inventory and management system;
- Enterprise risk may use an enterprise risk management system;
- Cyber Risk may use a TPRM tool;
- Security or IT operations may use a ticketing system to track vendor risk mitigation action items;
- And the CISO's office may use an IT GRC system to manage IT risk and report it to executive management.

Some enterprises opt to implement a full-featured system that contains all of the modules, while others may customize a flexible system or try tying together multiple systems. Here's one example of a workflow involving multiple systems:

Procurement implements an inherent risk questionnaire in the vendor management system, triggering a cyber-security assessment notification as appropriate. The system creates a data file of all new vendors, new contracts with existing vendors, contract renewals, and contract terminations.

Cyber Risk uses a TPRM system that imports the data export from the procurement system. The TPRM system provides a portal capability to allow vendors to answer assessment questionnaires online and consolidates the artifacts, audit results, and information from a security rating system into one pane of glass for assessors to analyze.

The TPRM system data is consolidated into an enterprise GRC system that's used to manage enterprise risk and report to various stakeholders.

It's important to map out the vendor management stakeholders, define the workflow, and make product and tooling decisions that make sense for your organization.

10.

Metrics and Reporting

A TPRM program's success can be measured through both Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs). The former provide evidence that the program is tangibly reducing the risk of vendor engagement; the latter that the program's process is improving in terms of efficiency—time and scale—and cost/money.

Some KRIs include:

- Percentage of vendors who fall below or above the business's risk tolerance thresholds
- Improvement in third-parties' overall risk
- Ongoing aggregate risk across the vendor portfolio and within subgroups of vendors providing similar services or goods

Some KPIs include:

- The time between when a LOB requests an assessment and the vendor is onboarded.
- The amount of time actively spent by assessors in reviewing a vendor.
- The number of assessments that can be supported in a given period (e.g., per month)
- The above, broken down by new and existing (reassessments, different contracts) vendors.

03

Conclusion

03 Conclusion

Third-party risk isn’t static, and your program can’t be either. The practices outlined in this guide are meant to help you build a resilient foundation and respond decisively when conditions change, whether that’s a new regulatory mandate, a CVE disclosure, or a shift in vendor behavior.

The key is to focus on what matters most: visibility, speed, and partnership. Don’t get caught in checkbox assessments that age out in weeks. Instead, aim for a program that’s defensible, measurable, and ready for the unexpected.

To see how one end-to-end solution can help you reduce risk, streamline assessments, respond faster to threats, and scale your TPRM program with confidence, visit Bitsight Third-Party Risk Management.

Visit Third-Party Risk Management

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is the global leader in cyber risk intelligence, leveraging advanced AI to empower organizations with precise insights derived from the industry’s most extensive external cybersecurity dataset. With more than 3,400 customers and 65,000 organizations active on its platform, Bitsight delivers real-time visibility into cyber risk and threat exposure, enabling teams to rapidly identify vulnerabilities, detect emerging threats, prioritize remediation, and mitigate risks across their extended attack surface.

BITSIGHT