axiom
corestream grc

Revolutionizing Third Party Risk Management - how to guide

Is the traditional vendor questionnaire still fit for purpose?

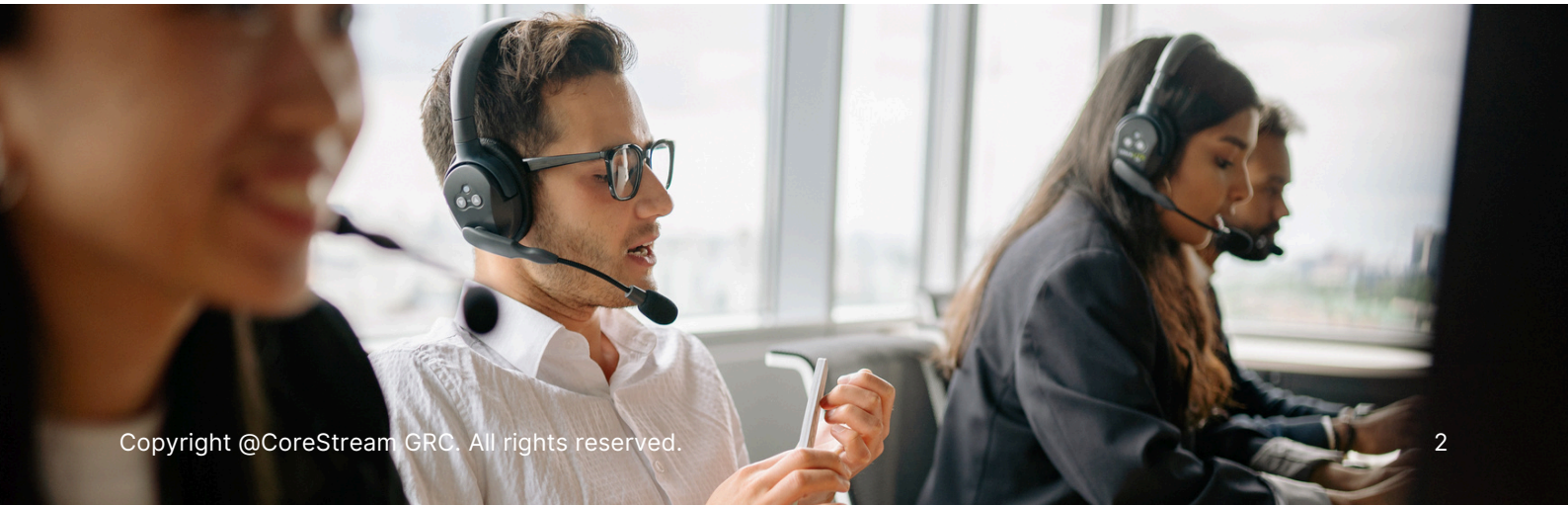
Imagine beginning a vendor assessment **without** sending another 200-question form.

Before contacting the third party, you already **understand who the organization is, who sits behind it, and whether there are public risk signals that warrant closer attention.** You can ask the vendor for the evidence it already holds, identify the gaps that genuinely matter, and stay alert to new risks as the relationship evolves.

That would change the starting point and the feeling of third-party risk management.

The pressure to find a **better approach** is growing. Organizations are managing more suppliers across a more complex regulatory environment, from DORA and NIS2 to GDPR, the EU AI Act, and sector-specific requirements. PwC's Global Compliance Survey 2025 found that **85% of respondents believe compliance requirements have become more complex over the past 3 years.**

At the same time, the risk does not stand still. Verizon's 2026 Data Breach Investigations Report found that **third-party involvement in breaches increased by 60%, with breaches involving a third party now accounting for 48% of all breaches.** The World Economic Forum reports that **65% of large companies identify third-party and supply-chain vulnerabilities as their greatest cyber-resilience challenge, up from 54% in 2025.**



Yet many teams are still trying to manage this expanding risk landscape through point-in-time questionnaires. The result is familiar:

- **More suppliers to assess**
- **More evidence to review**
- **More regulatory obligations to track**
- **More scrutiny from auditors and regulators**
- **More work competing for limited internal resources**

The scale of the problem is already visible. The UK National Cyber Security Centre says **only 14% of firms are on top of the potential risks posed by their immediate suppliers.** It also notes that relatively few organizations formally review cyber risks across their supply chains, often because they lack the capacity, capability, and tools to do so.

As Michael Rasmussen of GRC 20/20 observed after recent discussions with organizations facing these challenges:

> *"The scale is mind-blowing — lots of third parties — and the complexity even more so. Vendors are suffering from questionnaire fatigue, hit by duplicate assessments from every direction. Platforms are over-customized. Risk intelligence is powerful but fragmented across silos — cyber, financial, sanctions, sustainability — each in its own world."*
>
> Michael Rasmussen, GRC Analyst & Pundit

The question is not whether vendor questionnaires have value. It is whether they should still be doing so much of the **heavy lifting.**

Can you understand a third party before sending a questionnaire?

A stronger assessment begins with 2 layers of information.

The first is **vendor-provided evidence**: the policies, contracts, SOC reports, ISO certificates, audit reports, regulatory documentation, and proof of control operation that the third party already holds.

The second is **external intelligence**: the public and proprietary data that can help your team understand who the organization is, who controls it, how it is connected to other entities, and whether there are risk signals that require further investigation.

Together, these layers give you a more **useful starting point than a blank questionnaire.**

Instead of asking every vendor to manually restate information that may already be available, your team can focus on the gaps. **You ask fewer questions, but the questions are more relevant.** The vendor spends less time repeating basic information. Your team spends less time chasing responses and **more time applying judgment.**

According to Deloitte's third-party risk management guidance, **advanced analytics, AI, and experienced researchers can examine online and proprietary sources to identify risks associated with companies, key individuals, and ultimate beneficial owners.**

That is where the CoreStream GRC and Xapien integration supports a stronger due-diligence process. Xapien helps teams **gather and interpret external information**, uncover relevant context, distinguish between organizations and individuals with similar names, and surface potential red flags for human review.

As Emily Morgan, Global Partnerships Director at Xapien, explains:

> *"The volatile nature of today's global business landscape is driving organizations to ask 'should we do business with this partner' not 'can we?'"*

xapien

The speed difference is significant. Research that **previously required 8 analyst hours can now be completed in under 10 minutes.**

That is a partner-reported figure, but the wider value is clear. **Better external intelligence gives compliance teams a stronger foundation** before they decide what evidence to request, what questions to ask, and what needs closer attention.

What happens when the risk changes after onboarding?

A vendor assessment cannot stop when the onboarding form is complete.

Ownership structures change. Sanctions lists are updated. Adverse-media stories emerge. Cyber vulnerabilities develop. Certifications expire. **New evidence may strengthen the assurance picture, while fresh risk signals may require further investigation.**

This is where external data integrations become critical. They help turn a **static assessment into a more responsive view of risk.**

For example, the CoreStream GRC and LexisNexis integration brings real-time sanctions and adverse-media data into third-party due-diligence workflows. Rather than relying solely on information collected during onboarding, **teams can use trusted external data to identify emerging risk indicators and make faster, more informed decisions.**

Cyber risk requires the same ongoing visibility. The **CoreStream GRC and Black Kite integration** supports real-time cyber intelligence and continuous monitoring across vendors, partners, and suppliers. Black Kite can also **use existing intelligence and vendor documentation to support assessments, identify gaps, and help teams send focused questionnaires only where needed.**

As Eireann Connolly, CRO at Black Kite, explains:

"Managing cyber risk at scale demands more than automation."

BLACK KITE

2.0 What happens when the risk changes after onboarding?

The external-data layer is not limited to 1 provider. Through its configurable integration ecosystem, CoreStream GRC can connect with data sources including LexisNexis, D&B, ClarifiedBy, Cedar Rose, Neotas, Exiger, Threat.Digital, Black Kite, and other tools selected by the organization.

Different providers support different use cases. These can include **sanctions screening, adverse-media checks, corporate information, due diligence, cyber-risk intelligence**, and other third-party risk signals. The point is not to force every organization into the same data stack. It is to bring the **relevant intelligence into the workflow** so teams can respond when the risk changes.

Fresh intelligence should not automatically trigger another blanket questionnaire. It should help the organization **probe intelligently.**

A new risk signal may justify a targeted follow-up question. A change in ownership may require enhanced due diligence. An expired certification may trigger a request for updated evidence. A material cyber alert may need escalation and remediation.

That is a much **stronger model** than waiting for the next annual review.

How does better intelligence on your third parties give you time back?

Once your team has independently gathered ownership information, corporate linkages, and contextual risk signals, you no longer need to ask every vendor the same questions from scratch. You can **focus on what is missing, unclear, or genuinely material to the relationship.**

That matters as third-party networks grow. According to KPMG's 2026 Global Third-Party Risk Management Survey, **83% of executives plan to expand their partner networks over the next 1–3 years. At the same time, 48% see room for better collaboration on risk management.**

The answer cannot be to send more questionnaires to more vendors. A stronger Third Party Risk Management solution applies risk-tiering logic so that the depth of the assessment reflects the actual exposure. A critical technology provider with access to sensitive data may need a deeper review. A lower-risk supplier may require a lighter process. Where further questions are needed, they should be focused on the gaps that matter.

Can evidence replace lengthy control questionnaires?

In many cases, vendors have already done the hard work. They hold policies, procedures, contracts, SOC reports, ISO certificates, audit reports, and evidence that controls are operating in practice.

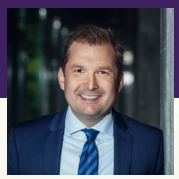
The traditional approach asks the vendor to translate that evidence into another lengthy questionnaire. The buying organization then manually reviews the answers and tries to map them back against its requirements. This creates work on both sides and risks losing useful context along the way.

There is a more **efficient** option. Ask the vendor for the evidence it already holds, then assess that evidence against the framework, regulation, or standard that matters to your organization.

The SANNOS and CoreStream GRC partnership is designed around that **evidence-first approach**. SANNOS reads real artifacts, maps them against defined requirements, identifies areas of conformance and non-conformance, and generates traceable outputs that teams can review and act on.

"Most compliance pain is not strategy. It's reading, mapping, and proving."

Anders Søborg, Co-CEO



SANNOS.

The aim is not to automate judgment. It is to **remove the manual reading, mapping, and chasing** that prevents experienced teams from applying their judgment where it adds the most value.

Why should vendors be able to reuse credible evidence?

A policy, certification, or audit report should not need to be manually rewritten every time a new client asks a slightly different version of the same question.

The UK National Cyber Security Centre makes this point directly in its Cyber Essentials Supply Chain Playbook. It says suppliers **can use Cyber Essentials certification as evidence across their customer base, reducing the time spent completing duplicative questionnaires.** The NCSC Annual Review 2025 also reports that 48% of respondents saved time on cyber security due diligence where a potential supplier was Cyber Essentials certified.

There is a wider security benefit too. In the playbook, St James's Place reported a significant fall in incidents after introducing Cyber Essentials across its supply chain:

> *"Security incident numbers have significantly reduced. We have seen around 80% reduction in cyber security incidents."*
>
> Matthew Smith
> Divisional Director of Cyber Security, St James's Place

A certification does not replace all due diligence. Nor does a SOC report, policy, or audit record. But **credible evidence should reduce the need to ask vendors to repeatedly describe controls they have already documented and tested.**

Is the vendor risk assessment questionnaire dead, then?

Not entirely. But the blanket questionnaire is losing its place as the default starting point for every vendor assessment.

A questionnaire remains useful where information cannot be verified independently, evidence is missing, or a risk-based assessment identifies a specific gap. The difference is that the **questions should now follow the risk**. Teams should not be asking every vendor to complete the same lengthy form when **existing intelligence and evidence can already provide many of the answers.**

That is consistent with the US Department of Justice's guidance on corporate compliance programs, which says **organizations should apply risk-based due diligence to third-party relationships and continue managing those risks throughout the lifespan of the relationship.**

"The questionnaire is not dead. But the blanket questionnaire is. The future is targeted, evidence-first, and proportionate to risk."

Paul Cadwallader, GRC Strategy Director

corestream grc

What does a stronger model for vendor risk assessment look like?

A modern vendor risk assessment should not begin and end with a questionnaire. Vendors should instead take ownership and create a living third-party assurance pack that develops over time as new evidence, certifications, reports, and risk signals emerge.

The UK National Cyber Security Centre recommends **taking a proportionate approach to supplier risk, with requirements tailored to the size, type, and risk profile of the supplier.** That principle should shape the full assessment process:

1. **Start with independent intelligence.** Use structured datasets and public-source information to build an initial view of the third party before asking questions.
2. **Understand who you are dealing with.** Identify ownership structures, beneficial owners, key principals, corporate linkages, and relevant red flags.
3. **Apply risk tiering.** Consider the service provided, access to data or systems, geography, criticality, and the potential impact of disruption or misconduct.
4. **Request the evidence that matters.** Ask the third party for relevant policies, procedures, certifications, contracts, audit reports, and proof that controls are operating in practice.
5. **Assess the evidence against defined requirements.** Map the material against the relevant framework, regulation, standard, or internal control baseline.
6. **Ask targeted follow-up questions.** Focus on the missing evidence, unclear answers, and risk signals that genuinely require clarification.
7. **Keep the assessment alive.** Record decisions, exceptions, remediation actions, approvals, and ongoing monitoring inside CoreStream GRC so teams can respond as evidence and risk signals change.

This is **value-based GRC in practice**. The aim is not simply to complete an assessment faster. It is to **improve the quality, consistency, and defensibility of the decision.**

Conclusion: Replace repetitive questionnaires with better questions and greater insights

Organizations should still ask vendors questions. But they do not need to ask questions that existing intelligence and credible evidence can already answer.

A stronger vendor risk management program starts with **independent intelligence, assesses the evidence already available, and uses targeted questions where further clarification is genuinely needed.** This helps teams reduce assessment fatigue, shorten onboarding timelines, and apply their judgment to the risks that matter most.

The process should not stop once the vendor is approved. Certain changes, including sanctions updates, can already be identified as they emerge. Other forms of deeper ongoing due diligence, such as identifying new litigation or adverse-media developments, are continuing to evolve. The goal is to build a stronger foundation for monitoring risk throughout the relationship, with a clear process for reviewing new evidence and responding when material changes are identified.

The result is **better for both** sides. Vendors spend less time repeating information they have already documented. Internal teams spend less time chasing responses and manually interpreting evidence. And the organization gains a clearer audit trail, a more proportionate assessment process, and a structured way to manage third-party risk as new information becomes available.

Ready to move beyond blanket vendor questionnaires?

See how SANNOS, Xapien, and CoreStream GRC can help your team combine independent intelligence, evidence-based assessment, and auditable workflows in **1 connected third-party risk management process.**

Request a demo

axiom
corestream grc

For more information please contact:

Email us to book your demo:
demo@corestreamgrc.com

corestreamgrc.com

Book a workshop

TPRM solution

Follow us on LinkedIn