How to Develop Effective Information Gathering for Third Parties

A 2026 Guide to Vendor Due Diligence and Stronger TPRM Governance

SURECLOUD®

www.surecloud.com

SURECLOUD®

GDPR Compliant

teiss Awards Winner Best Security Compliance Product

WINTER 2026 High Performer ENTERPRISE

SPRING 2026 Best Est. ROI ENTERPRISE

WINTER 2026 EMEA High Performer

Table of Contents

Highlights

- A practical framework for structuring vendor information gathering across the full third party lifecycle
- Guidance on the five core categories of third party information: organisational and ownership, financial health, cyber security, compliance, and operational resilience
- A tier differentiated validation model showing what proportionate verification looks like for critical, important, and lower risk vendors
- Coverage of fourth party risk scoping, including how to gather information about processor exposure
- Current regulatory context across DORA, NIS2, and financial services outsourcing expectations, with live 2026 enforcement signals

Who should read this?

This guide is designed for senior leaders responsible for vendor governance and third party risk oversight, including CISOs, Heads of Third Party Risk Management, Vendor Risk Leaders, Heads of Risk and Compliance, Procurement Governance Leaders, and Internal Audit Directors. It is also relevant for vendor risk analysts, compliance teams, IT security governance teams, and procurement teams involved in improving third party risk oversight across the organisation.

What this guide helps readers do

This guide helps readers assess their current approach to vendor information gathering, understand the operating model weaknesses that limit assurance quality, and identify the practical next steps most likely to improve governance, resilience, and regulatory defensibility. It provides a structured way to evaluate how vendor identification, risk classification, due diligence design, evidence validation, and technology need to evolve as third party ecosystems become more complex and regulatory expectations continue to rise.

Executive Summary

Third party risk management is not a questionnaire problem. It is an information problem.

Organisations continue to onboard vendors without a reliable picture of their security posture, financial stability, or operational resilience. They complete due diligence at the start of the relationship and treat it as done. The result is oversight that looks complete on paper and fails under scrutiny.

The consequences are measurable. IBM's Cost of a Data Breach Report 2025 found that supply chain compromise accounted for approximately 15 percent of initial attack vectors studied, at an average cost of $4.91 million per incident, and took 267 days to detect and contain, the longest of any vector. Verizon's 2025 Data Breach Investigations Report found that third party involvement in confirmed breaches doubled in a single year, rising from 15 to 30 percent.[1] [2]

These are the costs of information gaps that structured due diligence should catch early.

Regulation has moved in the same direction, and 2026 is the year it bites. DORA has been in force since January 2025, and national supervisors are now scrutinising ICT third party registers rather than waiting for them. NIS2's full compliance deadline is October 2026, bringing manufacturing into scope for the first time and extending supply chain obligations to suppliers of in scope entities. The UK's Critical Third Parties regime is expected to make its first designations during 2026. Personal liability for management is now explicit under both DORA and NIS2.[3] [4] [5] [6]

Most third party due diligence programmes are still built around manual questionnaires, inconsistent assessment practices, and limited evidence validation. That model was never strong. Against the current environment, it is no longer defensible. Organisations that invest in structured, lifecycle aware information gathering will identify vendor risk earlier, make governance decisions they can defend, and respond faster when a vendor's risk profile changes. Those that do not will find it harder to satisfy regulators or avoid consequences they could have seen coming.

This guide sets out how to rebuild the foundation.

1. The Third Party Risk Environment and Why Programmes Fail

Effective information gathering matters because the third party risk environment has changed. Risk is no longer limited to a manageable set of known suppliers providing clearly defined services. It now spans a wider ecosystem of vendors, platforms, processors, and technology dependencies embedded in how modern organisations operate.

Digital Supply Chains and the Expansion of Third Party Dependency

Most organisations now rely on third parties not just for peripheral services but for core operational and digital capabilities. Cloud infrastructure, SaaS platforms, managed security services, data processing providers, payment processors, software development partners, and logistics and fulfilment networks have become embedded dependencies rather than optional suppliers. A breach or outage at any of them is an incident at the organisation.

Fourth Party Exposure and Processor Risk

The risk does not stop at direct vendors. Organisations increasingly face exposure through fourth parties: the processors, cloud hosts, software components, and specialist providers that their critical vendors themselves depend on. A supplier can pass security assessments and still introduce material risk through its own supply chain.

DORA requires financial entities to register outsourcing arrangements that support critical or important functions, extending visibility obligations beyond the direct contractual boundary. NIS2 takes a comparable approach for a wider range of sectors, requiring supply chain security measures that account for the security practices of direct suppliers and service providers. ENISA's 2025 Technical Implementation Guidance on NIS2 security measures sets out practical expectations for supply chain security policies, supplier vetting, and ongoing monitoring that national supervisors are expected to use as a reference point.[3] [4] [5]

In both frameworks, oversight is expected to extend beyond the first vendor relationship.

Regulatory Expectations Around Vendor Governance

Regulatory frameworks governing third party risk have moved from guidance to obligation. DORA Article 28 requires financial entities to manage ICT third party risk as part of their ICT risk management framework, with proportionality determined by the nature, scale, and criticality of each dependency. Article 28(4) requires a risk assessment and suitability evaluation before entering any arrangement, with more extensive obligations where the service supports a critical or important function. Article 28(3) establishes the Register of Information, which many national authorities required in xBRL CSV format for the first time in Q1 2026. The EBA Guidelines on Outsourcing Arrangements set parallel expectations for financial entities and require due diligence covering business reputation, expertise, financial resources, and organisational structure. The EBA is now consulting on broader expectations for the sound management of third party risk beyond traditional outsourcing arrangements.[3] [6] [7]

NIS2 extends supply chain security obligations under Article 21 to 18 sectors defined in Annexes I and II, including manufacturing, digital infrastructure, and energy. Fines run to €10 million or 2 percent of global turnover for essential entities and €7 million or 1.4 percent for important entities, with personal liability for management under Article 20.[4]

In regulated sectors, the standard is shifting. It is no longer enough to show that vendors were assessed at onboarding. Third party risk has to be understood, tiered, governed, and monitored across the lifecycle, and the evidence has to be current enough to defend in a supervisory review.

Many organisations are operating in this harsher environment with due diligence models that have not kept pace. That is where the real gap appears.

Incomplete Vendor Inventories

The most common and most consequential weakness in third party information gathering is an incomplete vendor inventory. Organisations frequently do not have a reliable, governed view of their full third party population. Vendors are onboarded through different business functions, procurement channels, and technology procurement routes without consistent registration or oversight. Shadow procurement and departmental purchasing decisions mean that critical suppliers may not be visible to the risk or compliance function at all.

Over Reliance on Static Questionnaires Without Tiering

The standard approach to third party due diligence remains the questionnaire, and questionnaires are not inherently flawed. The problem is how they are typically used. In lower maturity programmes, the same questionnaire is sent to every vendor regardless of the nature, criticality, or risk profile of the relationship. A cloud infrastructure provider processing sensitive customer data receives the same set of questions as a low value service supplier with no data access. High risk relationships end up under scrutinised. Lower risk vendors face unnecessary burden. Response quality and programme efficiency suffer equally.

Without risk based tiering, questionnaires generate activity rather than assurance. Process completion becomes the measure of success rather than genuine risk visibility.

Poor Evidence Validation

Collecting information from vendors is not the same as verifying it. Many organisations accept self attestation responses at face value without cross referencing them against certifications, audit reports, contractual commitments, or independent testing. A vendor that attests to ISO 27001 certification, regular penetration testing, or mature incident response capabilities may or may not be providing an accurate picture. Self attestation accepted at face value is not assurance. It is the appearance of assurance.

Lack of Lifecycle Thinking

Perhaps the most significant weakness in vendor due diligence is the treatment of information gathering as a one time activity. Organisations invest effort in onboarding due diligence and then treat the vendor as assessed. That assumption does not reflect how vendor risk actually behaves. Security postures change. Processor arrangements change. Financial conditions change. Key personnel change. Regulatory exposure changes. A vendor that presented a strong risk profile at onboarding may look materially different eighteen months later, and under a periodic review model those changes may not be identified until they have already created exposure. The EBA Guidelines on Outsourcing Arrangements make this expectation explicit: ongoing performance monitoring across all outsourcing arrangements, not just at onboarding.[6]

2. The Foundations of Effective Third Party Information Gathering

Addressing these weaknesses requires a more structured approach to the full information gathering process, from vendor identification through risk classification to collection, validation, and ongoing oversight. These are the foundations that allow due diligence to function as genuine risk intelligence rather than a compliance exercise.

Vendor Identification and Scoping

Effective information gathering begins with a reliable view of the vendor population. Before any assessment activity can be proportionate, organisations need to know which third parties exist, what relationship category they fall into, and what data, systems, or operational functions they touch.

Vendor identification should be treated as a governed process, not a one off exercise. That means establishing clear ownership for maintaining the vendor register, defining consistent criteria for what constitutes a third party relationship that requires oversight, and creating mechanisms to capture new vendors at the point of onboarding rather than retrospectively. It also means periodically auditing the register against procurement records, finance systems, and contract repositories to identify relationships that may have been missed.

The scoping questions are straightforward. What services or products does this vendor provide? What data does it access or process? What operational dependencies does the organisation have on it? What would the impact be if the vendor failed to perform or experienced a significant security incident? The answers become the inputs into risk classification.

Risk Classification and Tiering

Risk classification is what makes information gathering proportionate. Not all vendors present the same level of risk, and applying the same depth of due diligence to every supplier regardless of criticality creates both gaps and unnecessary burden.

A workable tiering model distinguishes between vendor relationships based on a combination of factors: the sensitivity of data accessed or processed, the criticality of the service to operational continuity, the level of system access or integration involved, the regulatory obligations associated with the relationship, and the concentration risk created if the vendor is unavailable or compromised. Vendors can then be classified into tiers that determine the scope and intensity of information gathering required. Gartner's guidance on TPRM identifies risk based tiering as one of the most important capability improvements available to organisations looking to improve the effectiveness and efficiency of their vendor oversight.[8]

Risk Tier	Classification Triggers	Due Diligence Requirements
Critical Tier 1 Annual review	**Core system or network access** Processes sensitive PII, PHI, or financial data at scale Single point of failure for operations or revenue High sub-processor or 4th-party exposure	Full security questionnaire (SIG / CAIQ) Penetration test evidence required On-site or remote audit (annual) Executive relationship owner assigned
High Tier 2 Annual review	**Significant data access, lower volume** Processes confidential or regulated data Supports important but non-critical business processes In-scope for GDPR, ISO 27001, NIS2, or DORA	SOC 2 / ISO 27001 certificate verification GDPR Data Processing Agreement required Abbreviated security questionnaire Business continuity assessment
Medium Tier 3 Biennial review	**Limited data access, non-critical process** Handles internal or semi-public business data Supports operational but not revenue-critical functions Low regulatory exposure, no direct system access	Self-attestation questionnaire Public certification spot-check Standard contract terms apply Review at contract renewal
Low Tier 4 Renewal review only	**No sensitive data or system access** Commodity or indirect service provider Minimal business dependency, easily substituted No regulatory in-scope obligation	Basic vendor registration form Financial stability check Standard terms and conditions apply No periodic review required

Classification is reviewed at onboarding, contract renewal, and on material change. Tier 1 and Tier 2 vendors trigger immediate re-assessment on breach notification.

Decision Oriented Information Requirements

Before designing assessments or sending questionnaires, organisations should be clear about what decisions the information gathered is intended to support. Information collection without a defined decision purpose generates volume without insight. The question at the design stage is not what information could we collect about this vendor, but what do we need to know in order to make a confident risk based decision about this relationship.

That framing changes the scope and structure of due diligence materially. It focuses collection on the information actually needed to assess the key risk dimensions of the relationship. It also makes it easier to define the threshold at which the information collected supports a risk acceptance, risk mitigation, or escalation decision.

The difference in practice is simple. An information question asks whether the vendor has a documented security policy. A decision question asks whether the organisation can accept the data processing risk this vendor introduces, given what it knows about the vendor's security management. That threshold definition transforms a questionnaire into a risk decision framework.

Understanding and Scoping Fourth Party Exposure

Fourth party risk, the exposure created by the vendors, processors, and technology dependencies of the organisation's direct suppliers, represents one of the most difficult challenges in third party information gathering. It cannot be ignored. DORA Article 28(3) requires Registers of Information to include outsourcing arrangements that support critical or important functions. NIS2 Article 21 extends supply chain security obligations beyond direct contractual boundaries.[3] [4]

The practical goal is not to eliminate fourth party exposure but to understand it well enough to manage the most material risks within it. For critical and important vendors, the assessment should include structured questions covering four areas.

Processor identification

Vendors should identify the processors, cloud infrastructure providers, software platforms, and specialist service providers on which the delivery of the contracted service depends.

Concentration and dependency risk

Vendors should identify single source dependencies for critical service components. In July 2024, a faulty CrowdStrike software update disrupted approximately 8.5 million Windows devices across thousands of organisations simultaneously. Direct vendor assessments would have shown no vulnerability. The failure was in the supply chain dependency itself.[9]

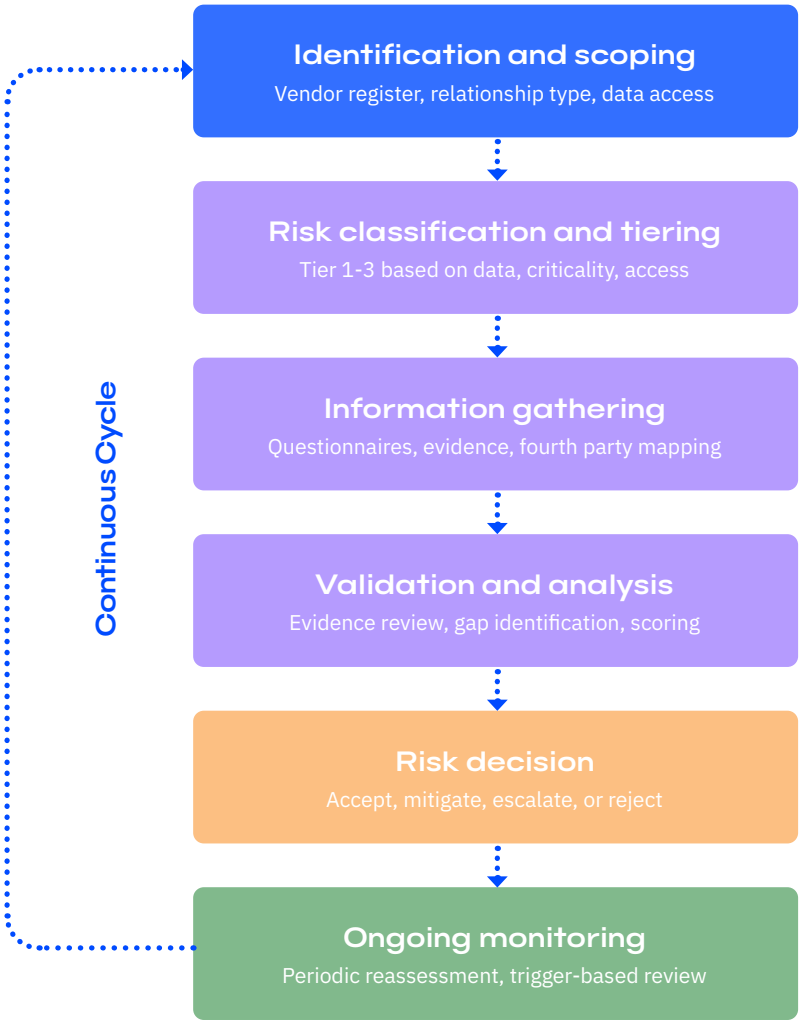
Processor security

Assessments should ask how the vendor governs the security practices of its own significant processors. A vendor with no visibility into its critical processors is a governance concern regardless of its own internal controls.

Notification obligations

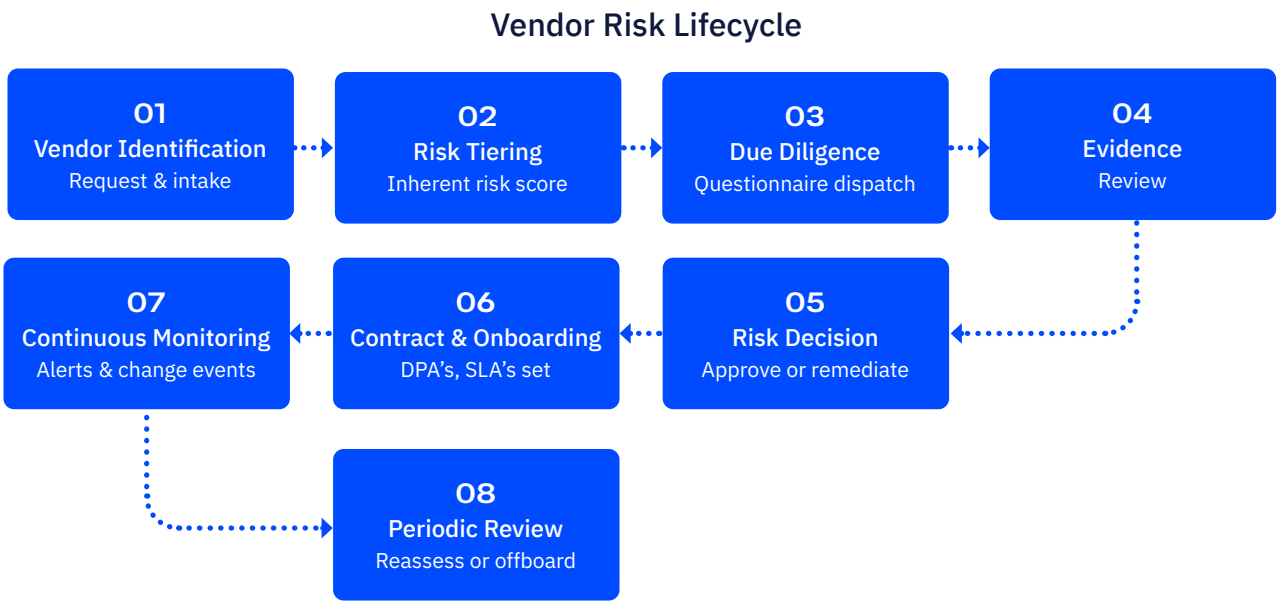
Contracts should require vendors to notify the organisation of material processor changes. DORA Article 28 and associated technical standards address this obligation for ICT third party service providers in financial services.[3]

For organisations subject to DORA, embedding fourth party information gathering into the standard assessment cycle is the most practical way to meet the Register of Information obligation and keep fourth party visibility current.



3. Key Categories of Third Party Information to Collect

Once scoping and tiering are established, the focus turns to what to collect. The five categories below represent the core domains of vendor risk assessment. The depth of collection within each should reflect the vendor's tier and risk profile.



1. Organisational and Ownership Information

Understanding who the vendor actually is forms the starting point of any due diligence process. This category covers the vendor's legal identity, corporate structure, ownership, and the relationships between related entities. It matters because organisational opacity, complex ownership structures, and undisclosed beneficial ownership can obscure conflicts of interest, regulatory exposure, sanctions risk, and the true accountability behind the services being provided.

Key information to collect includes the vendor's registered legal name and corporate structure, details of parent companies or affiliated entities, the identity of ultimate beneficial owners, any relevant regulatory registrations or licences, and any known or pending legal proceedings that could affect the vendor's ability to deliver services or its regulatory standing.

For higher risk relationships, this information also helps clarify where accountability sits if governance, resilience, or regulatory issues arise later in the lifecycle.

2. Financial Health and Stability

Vendor financial stability is frequently underweighted in due diligence. An operationally excellent vendor with deteriorating financial health represents a resilience risk that controls focused assessment will not identify.

Financial distress follows a predictable pattern. Security and infrastructure investment declines. Staff turnover increases as experienced people seek more stable positions elsewhere. Service quality deteriorates. By the time distress becomes visible as a service failure or vendor exit, the signals have typically been present for some time.

3. What to collect

Financial information to collect includes recent audited financial statements covering at least two to three years, credit ratings or reference data, revenue trends and profitability, evidence of financial reserves, and details of any material events including restructuring or ownership changes. For critical vendors, current debt levels and covenant positions are relevant, as covenant breaches can trigger rapid operational changes.

4. How to interpret what you collect

Three indicators matter most. Revenue concentration: a vendor heavily dependent on a small number of customers, or one where the organisation itself represents a material share of revenue, is more exposed to financial disruption. Liquidity: current ratio and cash flow from operations are more reliable indicators of short term resilience than net margin. Investment trends: a vendor consistently reducing technology spend relative to revenue is accumulating infrastructure debt that will eventually affect service quality. Where internal capability is limited, credit reference services or specialist providers can supply a structured assessment.

5. Cyber Security and Technology Controls

Cyber security is typically the most technically detailed domain of vendor due diligence. Core areas to assess include alignment to recognised frameworks such as ISO 27001:2022 and NIST CSF 2.0, access management and least privilege practices, encryption standards for data at rest and in transit, vulnerability and patch management, penetration testing frequency and scope, security incident response capabilities, and independent assurance artefacts such as SOC 2 Type II reports. For vendors with significant data access or system integration, extend the scope to development security practices, API and integration security, and the vendor's own supply chain risk management.[12] [13] [15]

Self reported responses should be validated against certifications and independent testing wherever possible. Technical assessment methods, including penetration testing, security architecture review, and continuous security monitoring via external intelligence platforms, provide a more reliable basis for assurance than attestation alone.

Three areas now warrant explicit coverage.

AI security governance

Ask whether vendors have formal policies governing AI tool usage, including controls over large language model access to customer data and shadow AI by staff. IBM's Cost of a Data Breach Report 2025 found that 13 percent of organisations reported breaches of AI models or applications.

Of those, 97 percent lacked proper AI access controls. The same report found that one in five organisations experienced a breach caused by shadow AI, at an average additional cost of $670,000.[1]

Cloud configuration security

Misconfigured cloud environments are consistently amongst the most common sources of vendor introduced risk. Assessments should cover cloud security posture management practices and access controls for cloud hosted customer data environments.

SaaS procurement governance

Vendors running large SaaS tool stacks without adequate oversight may be exposing customer data through platforms whose security posture they do not fully control. For high tier relationships, understanding how a vendor governs its own SaaS procurement is increasingly relevant.

Compliance and Regulatory Certifications

Understanding a vendor's compliance posture and the certifications it holds provides an important layer of assurance, but it requires careful interpretation. Certifications confirm that an organisation met a defined standard at a point in time and under specific scope conditions. They do not guarantee that the same standards are maintained continuously or that the certification scope covers the specific services being provided to the organisation.

Information to collect includes details of current certifications and their scope, validity periods, and certifying bodies. Relevant certifications will vary by sector and relationship type, but commonly include ISO 27001:2022, SOC 2 Type II, ISO 22301 for business continuity, and sector specific certifications relevant to the organisation's regulatory obligations.[13] [15]

Certification validation should go beyond accepting a vendor's statement that it is certified. Requesting copies of certificates, confirming validity and scope with issuing bodies where possible, and reviewing certification audit summaries are all reasonable steps for high tier vendors.

Operational Resilience

Operational resilience information addresses the vendor's ability to maintain service delivery under adverse conditions and recover from disruptions in a manner that does not create unacceptable impact for the organisation.

Information to collect includes the existence and currency of business continuity plans and disaster recovery arrangements relevant to the services provided, recovery time and recovery point objectives and how they align with the organisation's own impact tolerances, the results of recent business continuity tests and any identified gaps or remediation actions, arrangements for geographic resilience and alternative service delivery in the event of a primary site failure, and processor arrangements that could affect resilience if a critical processor experiences disruption.

For critical vendors, resilience information is not supplementary. It is central to understanding whether service disruption can be contained within the organisation's own impact tolerances.

4. Standardised Questionnaires and Frameworks

Standardised questionnaire frameworks provide a structured and consistent foundation for vendor information gathering. They reduce the design burden associated with building assessments from scratch, improve comparability across vendors, and align with recognised industry practices in a way that supports both internal governance and external scrutiny.

The Role of the SIG and Similar Frameworks

The Standardised Information Gathering questionnaire, published by Shared Assessments, is one of the longest established cross industry standardised assessment frameworks in the TPRM field. The SIG is designed to help organisations assess vendor risk across multiple domains in a more structured and consistent way. The 2025 SIG update includes mappings to frameworks and regulatory expectations including DORA, NIS2, and NIST CSF 2.0.[10] [11]

Other frameworks serve complementary purposes. The NIST Cybersecurity Framework 2.0 provides a broadly recognised reference model for assessing vendor security posture across the domains of govern, identify, protect, detect, respond, and recover. ISO 27001:2022 provides a standards based framework for evaluating information security management systems. For organisations subject to NIS2, ENISA's 2025 Technical Implementation Guidance translates the European Commission's Implementing Regulation into practical measures and evidence examples, including for supply chain security. For organisations subject to DORA, the European Banking Authority's standardised templates for ICT third party risk are directly relevant to financial entity obligations.[5] [12] [13]

The value of standardised frameworks lies in their ability to create a common assessment language between organisations and their vendors, reduce duplication of effort, and provide a defensible audit trail of the questions asked, responses received, and evidence reviewed. ISACA's work on vendor risk assessment practices supports the use of standardised approaches as a basis for proportionate and consistent due diligence across different vendor tiers and relationship types.[14]

One practical point: the SIG Core contains 627 questions across 21 risk domains. The SIG is designed to be scoped by domain, tier, and regulatory mapping, not deployed in full. A critical cloud infrastructure provider warrants far broader scope than a lower risk service supplier. The value is in the question library and regulatory mappings, not in asking every vendor every question.[11]

Security and Compliance Questionnaires

Security questionnaires remain a core mechanism for collecting structured data about vendor security controls and governance practices. Used well, they create consistency across assessment cycles and make it easier to compare vendors against the same control expectations. Used badly, they become long, repetitive, and weakly aligned to the actual risk decisions the organisation needs to make.

Compliance questionnaires have a distinct purpose: to establish whether the vendor can meet specific regulatory, certification, contractual, or policy obligations relevant to the relationship. This may include sector rules, privacy requirements, continuity obligations, or customer assurance commitments. Compliance questionnaires should not simply duplicate security questionnaires. They should focus on evidence that the vendor can meet the external and internal obligations attached to the relationship.

The Limits of Questionnaires

Standardised questionnaires are necessary but not sufficient. They capture self reported information at a point in time. They do not detect control failures a vendor is unaware of, inaccuracies in self assessment, or changes in posture between cycles. Vendors completing multiple questionnaires under commercial pressure rarely optimise their responses.

Question design matters as much as question coverage. Ambiguous or overly broad questions generate responses that are difficult to analyse and easy to misinterpret. For high tier vendors, questionnaire design should reflect a clear understanding of what information is needed and why, with question scope calibrated to the specific risk profile of the relationship rather than drawn from a generic template. Excessively long or poorly structured questionnaires reduce response quality and produce lower value outputs than shorter, focused assessments. Scope should be reviewed periodically to ensure it remains proportionate to the decisions being made and the tier of vendor being assessed.

The right combination of assessment methods should be determined by the vendor's tier, the nature of the risk presented, and the assurance threshold required. Standardising that approach by tier, and documenting the rationale for the methods applied, creates a more defensible assurance model.

A completed questionnaire is not the same as a defensible assurance decision. The questionnaire is a data collection instrument. Validation is the assurance mechanism.

5. Validating and Verifying Vendor Information

Collecting information is the first step. Validating it is what transforms a compliance exercise into genuine assurance.

Self reported assessment responses carry structural uncertainty. Vendors face commercial pressure to present their position favourably. Respondents facing complex or unfamiliar questions take shortcuts rather than providing optimal answers. Neither reflects dishonesty in most cases. Both produce information that cannot be fully trusted without independent verification. Validation is the mechanism for managing that gap. What proportionate validation looks like in practice depends on the vendor's tier.

Tier 1: Critical Vendors

These are vendors where a failure would create material operational disruption, regulatory exposure, or significant data breach risk. Validation should be comprehensive and largely independent.

Request full certification documentation, not summaries. For ISO 27001, request the certificate with scope description and the most recent surveillance audit letter. For SOC 2 Type II, request the full report including the description of the service auditor's tests and results, not only the executive summary. Qualifications, exceptions, and management responses in these documents carry as much information as the clean opinions.[13] [15]

Commission independent technical assessment. For critical vendors with significant system integration or data access, questionnaire based assessment should be supplemented by penetration testing, security architecture review, or cloud configuration review conducted by an independent party. Where the vendor does not permit direct testing, external security intelligence platforms that continuously monitor observable signals such as exposed credentials, misconfigured assets, and known vulnerabilities provide a meaningful independent layer.

Validate financial information through independent sources. Credit reference data, filed accounts, and publicly available financial statements should be reviewed and cross referenced with the vendor's self reported financial position. For vendors whose financial stability is material to operational continuity, financial monitoring should be ongoing.

Conduct structured interviews or on site visits for the highest risk relationships. Structured conversations with key vendor contacts, including security leads and operational managers, surface context and nuance that documentation review alone does not provide.

Tier 2: Important Vendors

These are vendors where a failure would create significant but manageable disruption or where data access is material but not critical. Validation should be evidence based but does not require the same depth as Tier 1.

Request current certifications with scope confirmation. Verify that the scope of any certification covers the specific services being provided to the organisation, not a different part of the vendor's business. A vendor may hold an ISO 27001 certificate that covers its UK operations only, whilst the services it provides are delivered from a different geography or entity.

Review recent audit reports or assurance documents where available. SOC 2 reports, penetration test executive summaries, and business continuity test results are reasonable requests for important vendors. The objective is corroboration rather than comprehensive independent verification.

Use external security intelligence as a continuous signal. Security ratings and threat intelligence platforms are a proportionate validation tool for this tier. They identify deterioration in observable security posture between formal review cycles, which is where periodic assessment alone creates gaps.

Tier 3: Lower Risk Vendors

These are vendors with limited data access, no system integration, and low operational criticality. Validation should be lightweight and efficient.

Confirm certifications where claimed. A simple confirmation request to the issuing body or a check against published certification databases is sufficient for most Tier 3 vendors.

Monitor for material changes at a category level rather than individually. Tier 3 vendors do not typically warrant individual ongoing monitoring. However, the programme should have a mechanism to identify when a Tier 3 vendor's circumstances change materially, such as a significant ownership change, a publicly reported incident, or a regulatory finding, that would trigger reassessment or re tiering.

Handling Inconsistencies and Gaps

Where questionnaire responses are inconsistent with evidence reviewed, where certifications cannot be confirmed, or where independent intelligence contradicts what a vendor has reported, organisations need a defined process for handling the discrepancy. That process should include a structured mechanism for raising the finding with the vendor and requesting clarification or additional evidence, a defined escalation path where the inconsistency is material or unresolved, a documented record of how the discrepancy was investigated and resolved, and a governance decision about whether the relationship can proceed, should proceed with conditions attached, or should be escalated for senior review.

Where a vendor is unable or unwilling to provide satisfactory clarification of a material inconsistency, that itself is a risk signal. A vendor that cannot confirm the scope of its own ISO 27001 certification, or that provides an audit report covering a different legal entity from the one delivering the service, is demonstrating either poor internal governance or a reluctance to provide accurate information. Neither is consistent with the assurance standard a critical or important vendor relationship requires.

All validation findings, including inconsistencies identified, clarifications sought, and resolutions reached, should be recorded as part of the assessment record. That documentation is what allows the organisation to demonstrate, to internal governance and to regulators where required, that assurance was not simply assumed from vendor responses but was actively tested and verified.

Tier 1 – Critical Comprehensive & independent

Annual Review

- [ ] **Full certification documentation requested**
  ISO 27001 certificate + surveillance audit letter; SOC 2 Type Il full report including test results
- [ ] **Independent technical assessment commissioned**
  Penetration test, security architecture review, or cloud configuration review by independent party
- [ ] **Financial information validated through independent sources**
  Credit reference data, filed accounts, cross-referenced with self-reported position
- [ ] **Structured interview or on-site visit conducted**
  Security lead and operational manager interviews to surface context beyond documentation
- [ ] **Fourth party exposure mapped**
  Sub-processors, cloud hosts, concentration risk, and notification obligations confirmed
- [ ] **Al security governance assessed**
  LLM access controls, shadow Al policy, and Saas procurement governance reviewed

Tier 2 – Important Evidence-based

Annual Review

- [ ] **Current certifications requested with scope confirmation**
  Verify scope covers the specific services provided, not a different geography or entity
- [ ] **Recent audit reports or assurance documents reviewed**
  SOC 2 executive summary, penetration test summary, or business continuity test results
- [ ] **External security intelligence monitoring active**
  Security ratings platform tracking posture between formal review cycles
- [ ] **GDPR Data Processing Agreement in place**
  Confirmed before data sharing begins; processor obligations documented

Tier 3 – Lower risk Lightweight & efficient

Biennial review

- [ ] **Certifications confirmed where claimed**
  Confirmation request to issuing body or check against published certification database
- [ ] **Self-attestation questionnaire completed and filed**
  Standard contract terms applied; responses held on record
- [ ] **Category-level monitoring in place**
  Mechanism exists to flag ownership changes, public incidents, or regulatory findings triggering re-tier

All inconsistencies identified, clarifications sought, and resolutions reached must be recorded as part of the assessment record. Tier 1 and Tier 2 vendors trigger immediate reassessment on breach notification.

6. Technology as an Information Gathering Enabler

Technology accelerates mature processes. Applied to fragmented ones, it accelerates the fragmentation.

The sequencing is frequently reversed in practice. Organisations invest in vendor risk platforms before they have a reliable inventory, consistent tiering, or clear assessment methodology. Bad processes, scaled by technology, remain bad processes. The right sequence is simple: stabilise governance and process foundations first, then use technology to sustain what is already working at a scale that manual effort cannot maintain.

Automated Questionnaires

Automated questionnaires are one of the clearest ways technology improves information gathering. Instead of manually distributing assessments, chasing responses by email, consolidating answers in spreadsheets, and storing evidence in inconsistent locations, organisations can route assessments automatically by vendor tier and service type, track completion status, send reminders, and hold responses in a consistent structure for analysis. The value is not speed alone. It is consistency. Every vendor in a given tier receives the same baseline assessment, at the same standard, with the same follow up discipline. That improves comparability across the vendor population and reduces avoidable manual effort.

Centralised Vendor Risk Repositories

A centralised repository is the single most important technological foundation for lifecycle governance. Without it, information collected at onboarding cannot be maintained, reassessment findings are disconnected from the original baseline, and the organisation cannot build a view of how vendor risk has changed over time. With it, the entire vendor lifecycle operates from a single source of record.

A well designed repository holds vendor profile data, tiering classifications, assessment history, certification records with expiry tracking, evidence documentation with version control, remediation status, and issue tracking in a single governed structure. That connectivity makes reassessment more efficient, improves reporting quality, and supports the kind of longitudinal risk view that DORA Article 28(3) and NIS2 Article 21 increasingly expect organisations to be able to demonstrate.

The quality of data held in the repository is directly dependent on the quality of the processes feeding it. A repository populated with inconsistent, outdated, or poorly structured data creates the appearance of oversight without the substance. Structured data fields with defined validation rules, clear ownership for data maintenance, and regular data quality reviews are necessary conditions for the repository to deliver its intended value.

Risk Scoring and Prioritisation

Risk scoring translates the outputs of vendor assessment into a structured view of relative exposure across the vendor population. Rather than treating all assessment findings as equivalent, a scoring model applies weighting to different risk domains, evidence quality, and contextual factors such as data sensitivity and operational criticality to produce a composite indicator that supports prioritisation.

Used well, risk scoring helps leadership understand where the highest risk relationships sit and where remediation investment should be concentrated. It also helps manage large vendor populations where the volume of assessment data makes manual prioritisation impractical.

The limitations of risk scoring matter as much as its benefits. Scoring models are only as reliable as the data they draw on and the weighting assumptions embedded in their design. A model that scores documentation quality rather than control effectiveness will reward well prepared responses regardless of underlying security posture. A model with fixed weightings that do not reflect the organisation's actual risk profile will produce scores that look rigorous but do not represent genuine exposure accurately. Organisations should treat risk scores as a prioritisation input rather than a definitive risk verdict, and should review the model periodically to ensure its assumptions remain appropriate.

Continuous Monitoring and Intelligence Integration

Continuous monitoring represents the most significant capability shift available to mature information gathering programmes. Rather than relying solely on periodic assessments to maintain awareness of vendor risk, continuous monitoring uses external intelligence feeds, security ratings platforms, and event based triggers to provide ongoing visibility into changes in vendor posture between formal review cycles.

External security intelligence platforms monitor observable signals including exposed credentials, misconfigured assets, unpatched vulnerabilities, and dark web indicators associated with vendor domains. Financial monitoring tools provide comparable value for vendor financial health. News and regulatory monitoring identifies material events, including public incidents, enforcement actions, ownership changes, and significant operational disruptions, that may affect a vendor's risk profile and warrant reassessment or escalation outside the normal review cycle.

Continuous monitoring creates value only where the underlying programme is mature enough to act on the signals it generates. An alert about deteriorating vendor security posture means nothing without a defined process for assessing its significance, escalating where necessary, and updating the assessment record. The operational framework must be in place before the monitoring technology is deployed.

Dashboards and Reporting

A mature vendor risk dashboard makes continuous oversight visible to governance. It shows inventory coverage, tiering distribution, assessment status by tier, open findings with remediation progress, concentration risk indicators, and live security intelligence alerts.

For senior leadership it should answer three questions at a glance: do we know who our vendors are? Do we have current assurance over the ones that matter most? Where are our most significant unresolved risks? A platform that cannot surface those answers is providing data management, not risk governance.

7. Moving from Periodic Assessment to Continuous Monitoring

Periodic assessment models were built for a vendor environment that no longer exists. Fewer relationships. More static arrangements. Predictable risk profiles. None of those conditions hold today. The practical question is what continuous oversight actually requires.

Building Event Based Reassessment Triggers

The practical bridge between periodic assessment and continuous oversight is the event based reassessment trigger. Rather than waiting for the scheduled review cycle, organisations should define the events and signals that warrant earlier reassessment and build those triggers into their operating model.

Relevant triggers include notification of a security incident at a vendor, material changes in vendor ownership or corporate structure, significant changes to the services or processors supporting the relationship, deterioration in security intelligence signals, financial distress indicators, regulatory findings or enforcement actions against the vendor, and changes in the organisation's own risk appetite or regulatory obligations that affect the classification of the relationship.

Triggers should be documented, owned, and acted upon within defined timeframes. The governance model should be clear about who receives trigger alerts, what the expected response is, and how trigger based reassessment findings are incorporated into the ongoing vendor risk record.

Lifecycle Governance Across the Vendor Relationship

Continuous oversight is most effective when it is embedded within a structured governance model for the full vendor lifecycle, from initial scoping and onboarding through ongoing monitoring, reassessment, incident management, and ultimately vendor offboarding or transition.

Each stage has distinct requirements. Onboarding establishes the risk baseline. Ongoing monitoring tracks changes to it. Formal reassessment validates and updates the record at risk appropriate intervals. Incident management requires rapid information gathering on impact and vendor response. Offboarding requires verification that data has been returned or destroyed, access revoked, and contractual obligations discharged.

Treating information gathering as a lifecycle discipline changes the resourcing model, the technology requirements, and the governance structure of the TPRM programme. Assessment ownership needs to be defined at each lifecycle stage. Response timelines for trigger events need to be agreed and enforced. The record of what was collected, validated, and acted on needs to be current enough to defend under regulatory scrutiny.

DORA requires financial entities to apply ongoing oversight to critical third party relationships as part of their ICT risk management framework. NIS2 requires entities to implement and assess cybersecurity risk management measures that include supply chain security. Both point in the same direction: mature programmes do not stop at onboarding. They combine due diligence with ongoing oversight across the vendor lifecycle.[3] [4]

Conclusion

Third party information gathering is not an administrative task. It is the intelligence foundation on which sound vendor governance depends. When that foundation is weak, organisations are managing risk they cannot see clearly. When it is strong, they identify exposure earlier, make decisions they can defend, and adapt faster when a vendor's risk profile changes.

The framework in this guide builds in sequence. A reliable vendor inventory makes risk based tiering possible. Tiering makes assessment proportionate. Proportionate assessment produces information worth validating. Validation produces assurance that can be defended. Technology sustains it at scale. Each element depends on the ones before it. Automation applied to a weak foundation does not create maturity. It creates faster fragmentation.

The most useful next step is to identify honestly where the current programme sits against the foundations in this guide. Where is the vendor inventory incomplete? Where is tiering inconsistently applied? Where are responses accepted without validation? Where does oversight stop at onboarding? Those questions define improvement priorities more usefully than any generic roadmap. Inventory completeness comes first. Tiering determines what depth of assessment each vendor warrants. Validation improves quality before new collection is added. Technology scales what is already sound.

Third party risk will not become simpler. Ecosystems will continue to expand. Regulatory expectations will continue to rise. The supply chain will continue to be a primary attack surface. The organisations that govern that environment with confidence are the ones that treat information gathering as a lifecycle discipline, not a periodic exercise.

References

1. IBM and Ponemon Institute. Cost of a Data Breach Report 2025. IBM, 2025.
2. Verizon. 2025 Data Breach Investigations Report. Verizon Business, April 2025.
3. Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector (DORA), Articles 28 and 30. Official Journal of the European Union, 2022.
4. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2), Articles 20, 21 and 26, Annex I and Annex II. Official Journal of the European Union, 2022.
5. European Union Agency for Cybersecurity (ENISA). Technical Implementation Guidance on the Cybersecurity Risk Management Measures of the NIS2 Implementing Regulation. ENISA, June 2025.
6. European Banking Authority. Guidelines on Outsourcing Arrangements. EBA/GL/2019/02, 25 February 2019.
7. European Banking Authority. Consultation on Draft Guidelines on the Sound Management of Third Party Risk. EBA, 8 July 2025.
8. Gartner. Third Party Risk Management (TPRM): A Complete Guide. Gartner, 2024.
9. Microsoft. Helping our customers through the CrowdStrike outage. Microsoft, 20 July 2024.
10. Shared Assessments. About the SIG. Shared Assessments, 2025.
11. Shared Assessments. New in the 2025 SIG Update. Shared Assessments, 2025.
12. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.
13. International Organization for Standardization. ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection. ISO, 2022.
14. ISACA. Vendor Risk Assessments: Do Organisations Still Need Them? ISACA Now Blog, 2025.
15. AICPA and CIMA. SOC 2: SOC for Service Organisations. AICPA, 2024.

For more information on how SureCloud can assist your organization, visit us online at **www.surecloud.com**, or email **sales@surecloud.com**

SureCloud Summary

SureCloud Ltd. has two decades of experience as a leading provider of Governance, Risk, and Compliance (GRC) solutions since its founding in 2006. Headquartered in the UK, with offices in the US, SureCloud supports a global portfolio of organisations with its holistic and intelligent GRC platform. Whether addressing cyber risk, data privacy, third parties, or compliance demands, SureCloud has a proven record of empowering organisations to continuously identify, manage and automate their risk and regulatory alignment.

Corporate Headquarters 1 Sherwood Street, London, W1D 7HR