FOURTHLINE

FOURTHLINE | SOLUTION GUIDE

Third Party Risk Management

A Practitioner's Guide for COOs, CROs, and SMF24 Holders
FCA and PRA Regulated Financial Services Firms

01 OPERATING CONTEXT

Third-party risk management has moved from a procurement discipline to a board-level regulatory obligation. For mid-tier UK financial services firms, the change is not gradual. It is structural, and the consequences of failing to keep pace are now personal for the individuals holding senior management functions.

The operating model of every mid-tier firm in the UK financial services sector depends on third parties. Cloud providers host critical infrastructure. Software vendors run core policy, trading, and payments platforms. Specialist outsourcers process claims, settlements, and client data. In many cases, the firm could not function for more than a matter of hours if a critical supplier became unavailable.

Regulators understand this dependency. Their response has been to require firms to demonstrate that they have actively managed it, not just documented it. The distinction matters. A firm that can produce a supplier register, a materiality assessment, a set of exit plans, and a schedule of due diligence reviews is not necessarily a firm that has managed its third-party risk. What regulators want to see is evidence that those instruments work: that the register is accurate, the materiality criteria are applied consistently, the exit plans have been tested, and that the firm genuinely understands what would happen if its most critical suppliers failed.

The regulatory landscape shifted materially again in March 2026. The FCA published PS26/2, the PRA published PS7/26, and the Bank of England published its parallel policy statement for financial market infrastructures, creating a unified UK framework for operational incident reporting and material third-party arrangement reporting. These rules take effect on 18 March 2027. They extend the regulatory visibility of third-party dependencies beyond what any previous UK framework has required, and they impose direct supervisory reporting obligations on firms' material third-party arrangements as a standing annual obligation. The TPRM programme that was adequate under SS2/21 alone is no longer adequate. Firms have twelve months to prepare.

Mid-tier firms face a specific challenge that their larger peers do not. They carry the same regulatory obligations, the same supervisory scrutiny, and in many cases the same supplier concentration risk as major institutions, but with materially smaller compliance and risk functions. The capacity to build a third-party risk management programme from first principles while managing day-to-day operations does not exist in most mid-tier organisations. The result is a pattern FourthLine sees consistently: programmes built around documentation rather than capability, registers maintained by procurement rather than owned by first-line risk, and exit plans that have never been stress-tested against a realistic failure scenario.

This guide is for the COO, CRO, or SMF24 holder who carries personal accountability for the firm's third-party arrangements. It sets out the regulatory framework, the common failure modes, and the programme approach FourthLine uses to build TPRM capability that withstands supervisory examination.

02 REGULATORY DRIVERS

The regulatory framework governing third-party risk management for UK financial services firms is not a single instrument. It is a set of overlapping obligations, each with specific scope, requirements, and supervisory expectations. The senior manager accountable for outsourcing needs to understand how they interact, not just what each one says.

PRA SS2/21: Outsourcing and Third-Party Risk Management

PRA Supervisory Statement SS2/21, published in March 2021 with a 31 March 2022 implementation deadline, is the primary framework for PRA-regulated firms. It applies to banks, building societies, insurers, and investment firms authorised by the PRA. Its scope is broad: SS2/21 covers all outsourcing arrangements and, critically, extends requirements to other third-party arrangements where the firm's operational resilience or its ability to deliver important business services could be affected.

The core obligations under SS2/21 include the following. Firms must maintain a comprehensive register of all outsourcing and material third-party arrangements. They must apply documented materiality criteria to classify arrangements and calibrate the intensity of risk management accordingly. They must conduct appropriate due diligence before entering into material arrangements and on an ongoing basis throughout the relationship lifecycle. They must ensure contracts contain minimum provisions including access and audit rights, business continuity requirements, and step-in rights. For each material outsourcing arrangement, firms must develop, maintain, and test a documented exit strategy covering both stressed and non-stressed exit scenarios. The PRA is explicit: exit plan testing must assess operational and financial feasibility, not merely confirm that documentation exists. Responsibility for compliance must be allocated to a named SMF holder.

SS2/21 also addresses the relationship between third-party risk management and operational resilience. Firms must ensure that outsourcing arrangements do not undermine their ability to remain within their impact tolerances for important business services. This creates a direct link between the TPRM programme and the firm's operational resilience self-assessment.

FCA SYSC 8.1: Outsourcing Obligations

For FCA-solo regulated firms, the primary outsourcing obligation sits in SYSC 8.1. The rule requires that when a firm relies on a third party for the performance of operational functions critical to the performance of regulated activities, it must take reasonable steps to avoid undue additional operational risk. SYSC 8.1.7 sets out that firms must retain sufficient expertise to oversee the outsourced functions and must ensure the service provider complies with relevant regulatory standards.

SYSC 8.1 is less prescriptive than SS2/21 in its detailed requirements, but the FCA's supervisory expectations, articulated through FG16/5 and subsequent Dear CEO letters, make clear that solo-regulated firms are expected to adopt proportionate but substantive TPRM programmes that address the full lifecycle from pre-engagement assessment through to exit planning and testing.

FCA SYSC 15A and PS21/3: Operational Resilience

The FCA's operational resilience rules, introduced through PS21/3 and codified in SYSC 15A, create parallel obligations with direct implications for third-party risk. SYSC 15A.2.9 requires that firms must ensure they can remain within their impact tolerances for each important business service in the event of a severe but plausible disruption. Where a third party supports delivery of an important business service, the firm must assure itself that its third-party arrangements do not create a vulnerability that would prevent it from meeting that requirement.

This is not simply a documentation requirement. Supervisors expect firms to demonstrate, through scenario testing, that their third-party dependencies have been identified, assessed, and managed in a way that protects IBS continuity. The 31 March 2025 deadline for demonstrating the ability to remain within impact tolerances has passed. Firms that have not embedded third-party resilience assurance into their scenario testing programmes are now carrying active supervisory risk.

FCA FG16/5: Guidance on Outsourcing

FCA FG16/5 provides supplementary guidance on outsourcing, with particular focus on proportionality and the governance expectations for firms that outsource significant operational functions. It addresses due diligence, contract terms, ongoing monitoring, and the management of cloud service arrangements. Although FG16/5 predates SS2/21, it remains relevant guidance for FCA-regulated firms and should be read alongside SYSC 8.1 and SYSC 15A.

FCA PS26/2 and PRA PS7/26: Operational Incident and Third-Party Reporting

Published on 18 March 2026, FCA Policy Statement PS26/2 and PRA Policy Statement PS7/26 represent the most significant structural change to the TPRM regulatory landscape since SS2/21. Together with the Bank of England's parallel statement for financial market infrastructures, they establish a unified UK framework for operational incident reporting and material third-party arrangement reporting that will take effect on 18 March 2027.

The third-party reporting dimension of PS26/2 and PS7/26 creates two new standing obligations that go materially beyond any previous requirement. First, firms must notify the FCA and, where applicable, the PRA before entering into any new material third-party arrangement, or before making any significant change to an existing one. This pre-contractual notification obligation fundamentally changes the governance process for bringing on new material suppliers: regulatory notification is now a step that must occur before contractual or operational commitments are finalised, not after the fact. Second, firms must maintain a register of their material third-party arrangements and submit it to the FCA annually, within 90 calendar days of the FCA opening the reporting window. Third-country branches are included in the register requirement.

The definition of a material third-party arrangement for the purposes of PS26/2 sits in the FCA Handbook, and firms are responsible for developing their own assessment processes as part of their TPRM policy. This is not a narrow definition limited to material outsourcing arrangements as understood under SS2/21. It covers outsourcing and non-outsourcing arrangements, including intra-group arrangements that depend on external providers. Firms that have drawn their materiality boundary tightly under SS2/21 may find that the PS26/2 population is broader.

The operational incident reporting framework introduced by PS26/2 and PS7/26 also has direct TPRM implications. An operational incident is defined as a single event or a series of linked events that disrupts the firm's operations such that it disrupts the delivery of a service to an end user external to the firm, or affects the availability, integrity, authenticity, or confidentiality of information or data relating or belonging to such an end user. Given that the majority of operational incidents in recent years have originated at third parties, the incident reporting framework is closely linked to third-party risk management. Where a supplier failure triggers an operational incident that meets the reporting threshold, the firm is required to submit an initial report within 24 hours of forming a reasonable belief that the incident is reportable. For payment service providers, the deadline is four hours from first detection. Internal incident management processes must be calibrated to these external reporting deadlines.

PS26/2 is also supported by two pieces of finalised guidance: FG26/3 on operational incident reporting and FG26/4 on material third-party reporting. FG26/4 provides the practical framework for how firms should implement the materiality assessment and reporting process. Both guidance documents should be read alongside the policy statement rules.

The PRA's companion publication PS7/26 is accompanied by a new Supervisory Statement SS1/26 on operational resilience incident reporting, and by an update to SS2/21. The update to SS2/21 aligns the outsourcing supervisory statement with the new reporting regime. Dual-regulated firms will make a single submission via FCA Connect for incidents meeting both FCA and PRA thresholds, but must assess the two sets of thresholds independently, as they are broadly aligned but not identical.

The European Banking Authority's Guidelines on Outsourcing Arrangements, effective from 30 September 2019, apply to EBA-regulated entities including credit institutions and investment firms. They set out detailed requirements across the outsourcing lifecycle, including governance, risk assessment, contractual terms, sub-outsourcing, and cloud services. For UK firms with EU-regulated entities or branches, EBA Guidelines continue to apply alongside UK regulatory requirements and must be addressed in an integrated programme approach.

Regulatory Accountability: The SMF24 Obligation

PRA SS2/21 requires firms to allocate responsibility for outsourcing and third-party risk management to a named Senior Management Function holder.

For most dual-regulated firms, this sits with the SMF24 (Chief Operations Officer) or an equivalent SMF.

PS26/2 and PRA PS7/26 reinforce this accountability. The pre-contractual notification obligation for new and materially changed third-party arrangements, and the annual register submission, require a governed process with clear ownership.

The SMF24 holder cannot discharge their personal accountability by approving a notification after the fact.

The individual named must be able to demonstrate to supervisors that they understand the firm's third-party risk profile, that the programme meets regulatory standards, and that the governance processes for notification, register management, and incident escalation are operating as designed.

A programme that exists on paper but has not been operationalised does not satisfy this obligation. Personal regulatory accountability is not discharged by approving a policy document.

03 BUSINESS DRIVERS

Regulatory compliance is the floor, not the ceiling. Firms that approach third-party risk management purely as a compliance exercise miss the commercial case for doing it properly. The business drivers for a mature TPRM programme are substantial and, in a number of cases, more immediately consequential than the regulatory ones.

Operational Continuity

The single most important commercial driver is the protection of operational continuity. Mid-tier firms typically operate with lean internal capabilities and significant dependence on a small number of critical suppliers. The failure, disruption, or underperformance of any one of those suppliers can translate directly into an inability to service clients, meet regulatory reporting obligations, or process transactions. Understanding that dependency, and maintaining credible plans to manage it, is not a regulatory nicety. It is a basic condition of operational viability.

Concentration Risk

Cloud concentration is the most visible current example of third-party dependency creating systemic risk. Firms that rely on a single hyperscale cloud provider, or on a single software vendor for their core platform, have created a concentration exposure that may not be visible to the board until it crystallises. A mature TPRM programme requires firms to identify this concentration explicitly, to assess its impact on important business services, and to maintain documented contingency arrangements that are realistic rather than aspirational.

M&A and Corporate Change

Third-party risk management capability is increasingly scrutinised in the context of mergers, acquisitions, and change of control transactions. A firm that cannot produce a well-structured supplier register, a current materiality assessment, and a coherent set of exit plans will face delay and uncertainty in any transaction that requires regulatory approval or counterparty due diligence. FourthLine has supported multiple firms through this challenge, including international insurance groups where M&A activity had outpaced the integration of third-party risk management programmes.

Supervisory Engagement

Supervisors are increasingly using TPRM as an entry point for broader operational resilience scrutiny. A Dear CEO letter, a Section 166 review, or a routine supervisory visit that identifies weaknesses in the TPRM programme can escalate quickly into a broader programme of remediation work with defined deliverables and timescales. Firms that can demonstrate a well-governed, evidence-based programme are in a significantly stronger position in those conversations than firms whose programme consists primarily of documentation.

Insurance Sector: Specific Business Drivers

In the insurance sector, third-party dependencies have additional complexity. Lloyd's participants and MGAs depend on delegated authority arrangements that create regulatory obligations under both FCA and Lloyd's oversight. Reinsurance arrangements introduce counterparty risk alongside operational dependency. Claims management outsourcing creates direct customer outcome risk that intersects with the FCA's Consumer Duty expectations. A TPRM programme for an insurer must address these sector-specific dimensions, not merely apply a generic financial services framework.

PS26/2: A New Commercial and Regulatory Driver

The publication of PS26/2 and PRA PS7/26 in March 2026 adds a further, immediate commercial dimension to the business case for TPRM investment. The pre-contractual notification requirement means that inadequate materiality assessment processes will create delays in bringing on new suppliers: if the firm cannot determine reliably whether an arrangement is material, it cannot meet its notification obligation before commitment. The annual register submission means that an incomplete or inaccurate supplier register is no longer merely a governance gap; it is a regulatory reporting failure with a defined annual consequence.

Firms that have deferred TPRM programme investment now face a firm deadline. The 18 March 2027 implementation date gives a twelve-month window to build the processes, governance, and data quality needed to comply with the new reporting obligations. For firms that have not yet built a well-governed TPRM framework, that twelve months is tight. A Diagnostic conducted now, followed by a structured remediation programme, is the most efficient path to compliance.

04 WHERE MID-TIER FIRMS ARE FALLING SHORT

FourthLine has conducted TPRM programme reviews, gap analyses, and remediation engagements across a range of mid-tier UK regulated firms, including insurers, challenger banks, specialist lenders, investment managers, and building societies. The patterns of failure are consistent. They are not the result of bad intent. They are the result of building programmes around documentation rather than capability, and of treating regulatory compliance as a one-time exercise rather than an embedded operational discipline.

Failure Mode 1: Registers That Are Not Registers
Most firms have something they call a supplier register or an outsourcing register. In a significant proportion of cases, it is a procurement spreadsheet that has been renamed. It may list suppliers and some headline contractual data, but it does not capture the regulatory information required by SS2/21 or SYSC 8.1: the materiality classification, the IBS dependency, the outsourcing determination, the risk rating, the due diligence status, the exit strategy reference, or the contract review date. Without this information, the register cannot be used as a risk management tool and cannot satisfy supervisory scrutiny.

Failure Mode 2: Materiality Criteria That Are Not Applied
Many firms have documented materiality criteria in their TPRM policy or framework. Fewer firms have applied those criteria consistently across their entire supplier population, and fewer still have recorded the rationale for individual materiality assessments in a way that could withstand a supervisory review. The most common weakness is the treatment of legacy arrangements: long-standing supplier relationships that pre-date the current regulatory framework and that have never been formally assessed against current materiality criteria.

Failure Mode 3: Due Diligence That Stops at Onboarding
Pre-engagement due diligence has improved across the sector, driven partly by procurement process requirements and partly by contract negotiation. Ongoing monitoring has not kept pace. Firms that can demonstrate a robust onboarding process frequently cannot demonstrate that the same rigour has been applied to existing arrangements on a periodic basis. Annual reviews are frequently late, delegated to junior staff, or satisfied by reviewing a questionnaire response without any challenge or escalation process.

Failure Mode 4: Exit Plans That Have Not Been Tested
This is the single most consistently identified gap in FourthLine's TPRM programme reviews. Firms can generally produce an exit plan document for material suppliers. They cannot generally demonstrate that it has been tested. The PRA's requirement is explicit: exit plans must be tested for operational and financial feasibility, including in stressed exit scenarios. A document that describes the steps that would be taken to transition to an alternative provider, but has never been reviewed against actual transition timescales, alternative provider availability, or data extraction feasibility, does not satisfy the regulatory requirement.

Failure Mode 5: First-Line Ownership That Does Not Exist
TPRM programmes in mid-tier firms are frequently owned by a second-line risk function, a compliance team, or a programme manager. The result is a programme that can produce documentation but cannot evidence genuine first-line accountability for supplier risk. SS2/21 and the broader operational resilience framework require that the business lines responsible for using supplier services take ownership of the risks those services create. Building that ownership requires a deliberate programme of framework design, role clarification, training, and governance integration that most mid-tier firms have not completed.

Failure Mode 6: No Connection to Operational Resilience

The third-party risk management programme and the operational resilience programme exist as separate workstreams in the majority of mid-tier firms. The connection is made in policy documents but not in practice. Third-party dependencies are not consistently reflected in IBS resource maps. Exit plan activation has not been tested as a scenario within the operational resilience testing programme. Sub-outsourcing relationships have not been assessed for their potential to undermine impact tolerances. These gaps are visible to supervisors and create compounding risk in the self-assessment process.

Failure Mode 7: Incident Management Processes Not Calibrated to Regulatory Deadlines

Most mid-tier firms have internal incident management processes. Few have calibrated those processes to the external reporting timelines that PS26/2 and PRA PS7/26 will require from 18 March 2027. The 24-hour deadline for submitting an initial report to the FCA and PRA, once a firm has a reasonable belief that an incident is reportable, is significantly tighter than the typical internal escalation and approval cycle at most organisations. Where the incident originates at a third party, the lag between the supplier becoming aware and the firm forming a reasonable belief can consume a significant portion of that window. Firms that have not redesigned their incident escalation and classification processes with the external reporting threshold in mind will breach the deadline before they are aware it has been crossed. This is a gap that requires immediate attention, and which cannot be resolved by policy amendment alone.

The Pattern Supervisors Are Looking For

Supervisors reviewing a TPRM programme are not looking for the thickest policy document or the largest supplier register.

They are looking for evidence that the programme is operating, not just existing.

Key questions: Is the register current and complete? Have materiality assessments been applied and documented? Has due diligence been conducted on schedule? Have exit plans been tested? Can the firm demonstrate first-line accountability?

From 18 March 2027, PS26/2 and PRA PS7/26 give the FCA and PRA direct supervisory data through the annual register submission and pre-contractual notifications. Firms that cannot answer the above questions with evidence will not only fail a supervisory visit; they will produce a register submission that flags the weakness automatically.

Firms that cannot answer these questions with evidence, not assertions, are carrying significant supervisory risk

05 THE REGULATORY FRAMEWORK ARCHITECTURE

A compliant and operationally effective TPRM programme is built around a defined framework architecture. The architecture organises the regulatory obligations into a coherent structure that can be implemented, governed, and evidenced. The following components are the minimum required for a programme that meets PRA and FCA expectations.

Strategy and Risk Appetite

The firm must maintain a documented third-party risk management strategy that articulates its approach to outsourcing and third-party dependency, the risk appetite it applies to third-party arrangements, and the governance structure through which that appetite is set, monitored, and escalated. The strategy must be approved at board level and reviewed at least annually. It must reflect the firm's actual operating model, not a generic statement of principles.

Policy and Standards

The TPRM policy sets the regulatory and organisational requirements that govern all third-party arrangements. It must address: scope and definitions; roles and responsibilities across the three lines of defence; the lifecycle stages from pre-engagement through to exit; materiality and segmentation criteria; due diligence requirements by tier; minimum contractual provisions; ongoing monitoring and assurance requirements; exit planning and testing obligations; sub-outsourcing governance; and escalation and reporting requirements. Supporting standards and controls provide the operational detail beneath the policy framework.

Supplier Register and Segmentation

The supplier register is the foundational data asset of the TPRM programme. It must record all third-party arrangements within scope of the firm's regulatory obligations. Each entry must include, at minimum: the supplier name and service description; the outsourcing determination; the materiality assessment and classification; the IBS or critical function dependency; the inherent risk rating; the contract expiry and review dates; the due diligence status; the exit strategy reference; and the named first-line owner. Segmentation categories, typically strategic, critical, tactical, and transactional, must be applied consistently and documented with supporting rationale.

Due Diligence Methodology

The firm must maintain a documented due diligence methodology that calibrates the scope and depth of assessment to the materiality and risk classification of each arrangement. At minimum, due diligence must cover: operational and financial resilience; information and cyber security; data protection and data handling; business continuity and recovery capability; sub-outsourcing arrangements and concentration risk; regulatory compliance and right to audit; and financial viability. For material arrangements, due diligence must be conducted before entering into the arrangement and repeated on a risk-proportionate cycle during the life of the relationship.

Lifecycle Management

The TPRM programme must address the full supplier lifecycle. Pre-engagement: initial screening, due diligence, materiality assessment, contract negotiation, and approval. Onboarding: register entry, ownership assignment, monitoring framework activation. In-life management: periodic due diligence, performance monitoring, incident and escalation management, contract management. Exit: exit plan maintenance, testing, and activation. Each lifecycle stage must have documented processes, ownership, governance checkpoints, and management information outputs.

Minimum Contractual Requirements

Material outsourcing contracts must include specific provisions required by PRA SS2/21 and, where applicable, the EBA outsourcing guidelines. These include: access and audit rights; business continuity and recovery requirements; sub-outsourcing notification and approval; data protection and data portability; step-in rights; termination and transition provisions; regulatory notification requirements; and service level standards with consequences for breach. For cloud services, additional provisions addressing data residency, data extraction, and service portability are required.

05 THE REGULATORY FRAMEWORK ARCHITECTURE

Operational Incident Management and Regulatory Reporting

PS26/2 and PRA PS7/26, effective 18 March 2027, require firms to integrate external regulatory reporting into their incident management and TPRM frameworks. The framework must address three specific obligations. First, the pre-contractual notification process: before entering into a new material third-party arrangement, or before making a significant change to an existing one, the firm must notify the FCA and, where applicable, the PRA. The governance process for new and changed material arrangements must include a regulatory notification step before contractual commitments are made. Second, the annual register submission: firms must maintain a register of material third-party arrangements and submit it to the FCA each year within 90 calendar days of the reporting window opening. The register must be accurate, current, and complete. Third, incident reporting: where an operational incident, including one originating at a third party, meets the FCA and/or PRA reporting thresholds, the firm must submit an initial report within 24 hours. The internal incident classification and escalation process must be calibrated to this external deadline.

Firms that already maintain a well-governed TPRM register, with current materiality assessments and clear ownership, are well-positioned to meet the PS26/2 annual submission requirement. Firms that do not have this foundation will need to build it before March 2027. The register submission is not a new document: it draws directly on the firm's existing TPRM register. The quality of that register determines the quality of the submission.

Ongoing monitoring of material arrangements must be structured, scheduled, and evidenced. The monitoring framework should include: key risk and performance indicators reviewed at defined intervals; periodic due diligence refreshes aligned to the risk classification of the arrangement; incident and exception reporting from the supplier; access and audit rights exercised on a risk-proportionate basis; and escalation processes for performance deterioration or risk threshold breaches. Board and risk committee reporting must reflect the current state of the TPRM programme, including any open findings or remediation actions.

Exit Planning and Testing

For each material outsourcing arrangement, the firm must maintain a documented exit strategy that addresses both planned and stressed exit scenarios. The exit plan must: identify viable alternative providers or in-house transition options; assess the financial and operational cost of transition; address data extraction, system migration, and service continuity during transition; identify the critical path and minimum transition period; and specify the governance and decision-making process for triggering exit plan activation. Critically, exit plans must be tested. Testing must assess operational and financial feasibility, including in scenarios where the supplier is unavailable, in financial difficulty, or providing materially degraded service.

Framework Component	Regulatory Basis
TPRM Strategy and Risk Appetite	PRA SS2/21 Chapter 3; FCA SYSC 8.1
TPRM Policy and Standards	PRA SS2/21 Chapters 4-5; FCA SYSC 8.1.7
Supplier Register and Segmentation	PRA SS2/21 Chapter 5; FCA SYSC 8.1; PS26/2 (annual submission)
Due Diligence Methodology	PRA SS2/21 Chapters 6-7; EBA Guidelines Ch.5
Minimum Contractual Requirements	PRA SS2/21 Chapter 8; EBA Guidelines Ch.6
Ongoing Monitoring and Assurance	PRA SS2/21 Chapter 8; FCA FG16/5
Exit Planning and Testing	PRA SS2/21 Chapter 10; FCA SYSC 15A
Sub-Outsourcing Governance	PRA SS2/21 Chapter 9; EBA Guidelines Ch.7
Incident Management and Reporting	PS26/2; PRA PS7/26; PRA SS1/26; FG26/3
Material Third-Party Notifications and Register	PS26/2; PRA PS7/26; FG26/4 (effective 18 March 2027)
SMF Accountability	PRA SS2/21 Chapter 3; SMCR

06 FOURTHLINE'S PROGRAMME APPROACH

FourthLine has delivered TPRM programmes for mid-tier financial services firms since the regulatory framework began its current evolution. Our approach is structured around a four-phase delivery model that takes a firm from current-state assessment through framework design, implementation, and embedding. The model is calibrated to the size, complexity, and regulatory profile of each client, and is designed to produce regulatory evidence alongside operational capability.

Phase 1: Assess

Every FourthLine engagement begins with a structured assessment of the firm's current state against the regulatory framework requirements. We conduct a systematic review of the existing TPRM programme, including policy documentation, the supplier register, materiality assessments, due diligence records, contract management processes, monitoring outputs, and exit plan documentation. We benchmark the current state against the requirements of SS2/21, SYSC 8.1, PS26/2, and, where relevant, DORA, and produce a structured gap register with findings categorised by severity and regulatory obligation.

For firms with a March 2027 PS26/2 compliance deadline, the assessment includes a specific readiness review covering: the completeness and accuracy of the current supplier register against the PS26/2 materiality definition; the governance process for new and changed material arrangements, and whether it can accommodate the pre-contractual notification requirement; and the incident management framework, specifically whether internal classification and escalation processes are calibrated to the 24-hour external reporting deadline. These are not bolt-on additions to the gap analysis. They are part of the core assessment.

The assessment output is not a document review summary. It is a prioritised action plan that tells the firm's senior management exactly where the programme falls short of regulatory expectations, why that matters, and what is required to remediate it. Where a firm has a forthcoming supervisory engagement or self-assessment deadline, the assessment is structured to address that priority explicitly.

Phase 2: Design

In the design phase, FourthLine works with the firm to build or rebuild the core components of the TPRM framework. This includes: a TPRM strategy document aligned to the firm's actual operating model and risk appetite; a TPRM policy and supporting standards suite; a materiality and segmentation methodology with documented criteria and assessment tools; a TPRM lifecycle manual that defines the process, accountability, and evidence requirements at each lifecycle stage; a supplier register template populated with the firm's existing arrangements; and a due diligence questionnaire framework calibrated to the firm's supplier risk tiers.

FourthLine brings its own proven methodology toolkit, including a materiality and segmentation assessment tool, an ICT risk assessment framework, a supplier due diligence template library, and exit plan workbook templates. These are adapted to the firm's specific circumstances rather than delivered as generic products.

firm's SMF24 holder can stand behind.

Phase 3: Implement
Implementation translates the designed framework into operational reality. This is where mid-tier programmes most commonly fail without external support. Key implementation activities include: applying the materiality and segmentation methodology to the firm's full supplier population and completing the gap in the register; conducting or supervising the completion of due diligence for material arrangements where assessments are overdue or incomplete; reviewing and advising on contract uplift requirements for material arrangements that do not meet the minimum contractual standards; developing exit plans for material outsourcing arrangements; and establishing the ongoing monitoring and reporting framework including key risk and performance indicators.

For firms preparing for the PS26/2 effective date, Phase 3 also addresses the specific implementation requirements of the new reporting regime. This includes: designing and embedding the pre-contractual notification process for new and materially changed third-party arrangements, with governance checkpoints that ensure regulatory notification occurs before commitment; building the data collection and validation process required to produce the annual register submission; and redesigning the incident classification and escalation process to incorporate the 24-hour regulatory reporting deadline as a hard constraint, not a secondary consideration.

FourthLine's implementation approach uses a RACI model that builds first-line ownership from the start. We do not complete the work on behalf of the firm in a way that leaves no internal capability. We work alongside the firm's first-line risk owners, building their capability to maintain the programme on an ongoing basis.

Phase 4: Embed and Test
The embed and test phase is where FourthLine's work produces the evidence that matters most to regulators. We design and facilitate exit plan testing exercises for material outsourcing arrangements, using scenarios calibrated to the firm's specific supplier dependencies. Testing approaches range from structured desktop exercises to full simulation exercises that engage the firm's operational teams alongside supplier representatives.

We also support the integration of the TPRM programme into the firm's broader operational resilience testing cycle, ensuring that third-party failure scenarios are included in the severe but plausible scenario library and that the testing produces documented evidence of the firm's ability to manage supplier disruption within its impact tolerances. The output is a self-assessment-ready evidence pack that the firm's SMF24 holder can stand behind.

PHASE	**KEY DELIVERABLES**	TYPICAL DURATION
Phase 1: Assess	Gap register, prioritised action plan, regulatory benchmark	2-4 weeks
Phase 2: Design	TPRM strategy, policy, standards, lifecycle manual, methodology toolkit	4-8 weeks
Phase 3: Implement	Completed register, due diligence outputs, contract review, exit plan drafts	8-16 weeks
Phase 4: Embed and Test	Exit plan test exercises, scenario integration, evidence pack, SMF sign-off support	4-8 weeks

07 DORA: THE ICT THIRD PARTY DIMENSION

The EU Digital Operational Resilience Act (DORA) became effective on 17 January 2025. It applies to financial entities with regulated operations or entities within the European Union, including banks, insurers, investment firms, payment institutions, and electronic money institutions. UK firms with EU-regulated subsidiaries, branches, or qualifying EU-facing operations are in scope and must comply with DORA's requirements alongside their UK regulatory obligations.

DORA's third-party risk management framework represents the most prescriptive regulatory treatment of ICT supplier dependency yet introduced in any major jurisdiction. For firms in scope, it creates obligations that go materially beyond the requirements of PRA SS2/21 and FCA SYSC 8.1 in a number of areas. Understanding those differences is essential for any firm building an integrated TPRM programme.

Scope: ICT Third-Party Service Providers and Critical or Important Functions

DORA's third-party provisions focus specifically on ICT services. The relevant concept is the 'critical or important function', defined in Article 3(22) as a function whose disruption would materially impair the financial entity's compliance with regulatory requirements, its financial performance, or the soundness or continuity of its services and activities. This is broadly analogous to the concept of important business services under the UK operational resilience framework but is applied specifically in the ICT context.

Financial entities must identify which of their ICT services support critical or important functions and apply enhanced TPRM requirements to those arrangements. This identification process is itself a regulatory deliverable and must be documented and maintained.

Article 28: Policy on ICT Third-Party Risk

Article 28 of DORA requires financial entities to adopt and maintain a policy on ICT third-party risk as part of their ICT risk management framework. The policy must set out the principles, requirements, and processes that govern the use of ICT third-party services, including the criteria for determining which services support critical or important functions, the risk assessment approach, the contractual requirements, and the monitoring and exit planning obligations. The ESAs have developed regulatory technical standards that specify the detailed content requirements for this policy.

Article 29: ICT Concentration Risk

Article 29 introduces an explicit obligation to assess ICT concentration risk at entity level. Before entering into a contractual arrangement for ICT services supporting critical or important functions, the financial entity must assess whether the arrangement would involve an ICT third-party service provider that is not easily substitutable, or whether it would create multiple dependencies on the same provider or on closely connected providers. Where concentration risk is identified, the firm must weigh the benefits and costs of alternative solutions. This is a substantive analytical requirement, not a box-ticking exercise, and regulators will expect to see documented evidence of the assessment.

Article 30: Minimum Contractual Provisions

Article 30 specifies the minimum provisions that must be included in contracts for ICT services supporting critical or important functions. These go beyond the requirements of SS2/21 in several respects. They include: a full description of the services and the assets used or accessed; locations where services are provided and where data is processed; provisions on data accessibility, availability, and recovery; service levels with quantified performance targets; assistance obligations in the event of an ICT incident; security and access provisions; audit and inspection rights; sub-contracting notification and approval requirements; and exit strategy provisions including mandatory adequate transition periods. Firms reviewing legacy ICT contracts will in many cases need to renegotiate material terms to achieve DORA compliance.

Article 25: Testing Requirements Including ICT Third Parties

Article 25 of DORA requires financial entities to carry out appropriate testing of ICT tools and systems. Critically, this includes systems and tools provided by ICT third-party service providers that support critical or important functions. Testing must include scenario-based tests. For firms designated as significant under DORA's tiering framework, threat-led penetration testing (TLPT) requirements apply. The requirement to include ICT third-party service providers in the testing scope creates direct obligations for supplier engagement that many firms have not yet addressed.

Exit Strategies Under DORA

DORA Article 28(8) requires that for each ICT service supporting a critical or important function, financial entities must put in place exit strategies. These strategies must ensure that the firm can exit contractual arrangements without disruption to its business activities, without limiting its compliance with regulatory requirements, and without detriment to the continuity and quality of services provided to clients. Each contractual arrangement must include reference to exit strategies and establish a mandatory adequate transition period. Exit strategies must be developed, maintained, and tested where appropriate, particularly where the dependency, complexity, or lack of substitutability of the service increases risk.

The DORA Oversight Framework for Critical ICT Third Parties

DORA establishes a direct supervisory oversight framework for ICT third-party service providers designated as critical by the European Supervisory Authorities. The ESAs assess providers against criteria including their substitutability and the potential systemic impact of their failure, and appoint a Lead Overseer, which may be the EBA, EIOPA, or ESMA, for each designated provider. Lead Overseers have powers to request information, conduct investigations and inspections, and issue recommendations. Financial entities must cooperate with this oversight process and must take account of recommendations issued to their critical ICT providers.

DORA vs UK Framework: Key Differences

Concentration risk: DORA Article 29 requires an explicit entity-level assessment before entering into arrangements supporting critical or important functions. UK frameworks address concentration risk but without the same pre-engagement assessment obligation.

Mandatory transition periods: DORA requires that contracts include a mandatory adequate transition period. PRA SS2/21 requires testing for feasibility but does not mandate a specific contractual transition period.

ICT third-party testing: DORA Article 25 explicitly includes ICT third-party systems in the testing scope. UK frameworks address this through the operational resilience testing cycle but without equivalent specificity.

Direct oversight: The DORA oversight framework for critical ICT providers creates a regulatory dimension with no direct UK equivalent. Firms must monitor designations and respond to oversight findings affecting their suppliers.

08 DELIVERABLES

FourthLine's TPRM engagements are deliverable-led. Every engagement produces a defined set of outputs that the firm retains, owns, and can use as regulatory evidence. The following represents the standard deliverable set for a full TPRM programme engagement. Specific engagements are scoped to the firm's current state and immediate priorities, and not all deliverables will be required in every engagement.

Programme and Governance Deliverables

- TPRM Strategy Document: Board-level statement of the firm's approach to third-party risk management, aligned to its operating model, regulatory obligations, and risk appetite.
- TPRM Policy: Comprehensive regulatory-aligned policy document covering scope, obligations, lifecycle requirements, and governance structure.
- TPRM Standards and Controls Suite: Operational standards supporting the policy, including materiality and segmentation criteria, due diligence requirements by tier, monitoring standards, and exit planning requirements.
- TPRM Lifecycle Management Manual: Detailed process documentation covering each lifecycle stage with role accountabilities, process steps, approval requirements, and evidence standards.
- RACI Matrix: Cross-functional accountability map covering the three lines of defence across each lifecycle stage and governance function.

Assessment and Register Deliverables

- TPRM Gap Register: Structured assessment of the current programme against regulatory requirements, with findings categorised by severity and mapped to specific regulatory obligations.
- Completed Supplier Register: Fully populated register including outsourcing determinations, materiality classifications, IBS dependencies, risk ratings, contract data, due diligence status, and exit strategy references.
- Materiality and Segmentation Assessment Tool: Repeatable methodology tool with documented criteria and scoring mechanism for classifying new and existing arrangements.
- ICT Criticality Assessment: Assessment of ICT supplier arrangements against the critical or important function criteria, supporting both UK operational resilience obligations and DORA compliance.

Due Diligence Deliverables

- Due Diligence Questionnaire Framework: Tiered questionnaire library calibrated to the risk classification of each supplier arrangement, covering operational resilience, ICT security, BCM, data protection, financial viability, and sub-outsourcing.
- Due Diligence Assessment Reports: Completed assessments for material arrangements, including findings, risk ratings, and recommended actions.
- Cyber and Information Security Supplier Due Diligence Tool: Focused assessment tool for ICT suppliers, aligned to DORA Article 30 requirements and relevant cyber security standards.

Exit Planning Deliverables

- Exit Strategy Framework Document: Approach document setting out the exit planning methodology, scenario classification, testing requirements, and governance process.
- Exit Plan Templates: Structured workbook templates for material outsourcing arrangements, covering transition options, financial assessment, data extraction, critical path, and contingency measures.
- Completed Exit Plans: Developed and documented exit plans for named material arrangements, reviewed for operational and financial feasibility.
- Exit Plan Test Scenarios and Reports: Designed test scenarios for material arrangements, facilitated testing exercises, and post-exercise reports capturing findings, residual risks, and improvement actions

Monitoring and Reporting Deliverables

- KRI and KPI Library: Defined key risk and performance indicators for supplier monitoring, calibrated to the risk classification of each arrangement.
- Supplier Performance Monitoring Framework: Methodology for ongoing performance monitoring, including escalation triggers, review cycles, and reporting requirements.
- Board and Risk Committee Reporting Template: MI reporting template providing the TPRM programme overview, current risk profile, open findings, and emerging risks required for governance reporting.
- Third-Party Incident Management Process: Documented process for managing incidents involving third-party suppliers, including escalation, notification, and recovery steps.

DORA-Specific Deliverables

- ICT TPRM Policy (DORA-aligned): Article 28-compliant policy document covering the ICT third-party risk management requirements specific to DORA.
- Critical or Important Function Assessment: Documented assessment identifying which ICT services support critical or important functions, with supporting analysis.
- ICT Concentration Risk Assessment: Entity-level assessment addressing Article 29 requirements, including substitutability analysis and concentration exposure documentation.
- Contract Gap Analysis (DORA Article 30): Assessment of existing ICT contracts against the minimum provisions required by Article 30, with recommended contractual changes.

PS26/2 and PRA PS7/26 Readiness Deliverables

- Materiality Assessment (PS26/2 Scope): Review and, where necessary, redefinition of the firm's materiality criteria to align with the PS26/2 and FG26/4 definition of a material third-party arrangement, covering outsourcing and non-outsourcing arrangements including intra-group dependencies.
- Pre-Contractual Notification Process: Documented governance process for new and materially changed third-party arrangements, incorporating the FCA and PRA pre-notification step as a mandatory approval gate before contractual or operational commitment.
- Annual Register Submission Framework: Design and implementation of the data collection, validation, and submission process required to produce the annual material third-party register submission to the FCA, within the required 90-day window.
- Incident Classification and Escalation Redesign: Review and redesign of the internal incident classification and escalation process to incorporate the PS26/2 operational incident definition, the FCA and PRA reporting thresholds, and the 24-hour initial reporting deadline as binding process constraints.
- PS26/2 Readiness Assessment Report: Structured assessment of the firm's current readiness against the PS26/2 and PRA PS7/26 requirements, with a prioritised action plan for achieving compliance before the 18 March 2027 effective date.

Third-party risk management does not exist in isolation. A TPRM programme that is not connected to the firm's operational resilience programme, its business continuity management system, its ICT risk management framework, and its governance structures will produce documentation that satisfies individual regulatory obligations but fails to deliver the integrated capability that regulators are looking for. FourthLine's approach treats TPRM integration as a design requirement, not an afterthought.

Operational Resilience Programme

The connection between TPRM and operational resilience is the most important integration point. The firm's important business services depend on third parties for delivery. That dependency must be reflected in the IBS resource map. The potential failure of critical suppliers must be represented in the severe but plausible scenario library. Scenario testing must address third-party failure as a credible disruption event. The exit plans for material suppliers must be tested as part of the operational resilience testing cycle. Where these connections are absent, the firm's self-assessment will contain gaps that supervisors will identify.

FourthLine works to ensure that the TPRM programme and the operational resilience programme share a common view of the firm's critical supplier dependencies. We integrate the supplier register with the resource mapping process, design test scenarios that address supplier failure, and ensure that the evidence produced by TPRM activities contributes directly to the operational resilience self-assessment.

Business Continuity Management

Business continuity planning must address the risk of supplier disruption alongside internal disruption scenarios. Business impact analyses for important business services must capture third-party dependencies explicitly. Recovery strategies must address how the firm would maintain service continuity in the event of supplier failure, not just internal failure. For material outsourcing arrangements, SS2/21 requires firms to develop, maintain, and test business continuity plans that cover supplier disruption. These plans must be held alongside the exit plans for those arrangements and must be tested together.

FourthLine's BCM engagements are designed to work in concert with the TPRM programme. Where a firm is building or rebuilding both capabilities, we ensure the underlying data and analysis, particularly the criticality assessment and the dependency map, are shared across both workstreams rather than being developed in parallel and then reconciled.

ICT Risk Management and Cyber Resilience

The ICT risk management framework must address third-party ICT dependencies. The ICT criticality assessment must identify which systems and applications are provided by third parties, what the consequence of their unavailability would be, and what recovery arrangements exist. Cyber resilience obligations under the FCA's and PRA's operational resilience frameworks, and under DORA, require firms to understand the security posture of their critical ICT providers and to assure themselves that supplier-side vulnerabilities do not create unmanaged risk to the firm's important business services.

For firms in scope of DORA, the integration between the ICT risk management framework and the TPRM programme is a regulatory requirement. The ICT TPRM policy required by DORA Article 28 must be part of the broader ICT risk management framework, and the register of ICT third-party arrangements must be maintained as an integral component of the ICT risk management system.

Governance and SMF Accountability
Third-party risk management must be integrated into the firm's governance structure at multiple levels. The risk committee or board committee with oversight of operational risk must receive regular reporting on the TPRM programme, including the current risk profile, material open findings, and emerging risks. The named SMF holder responsible for outsourcing must have sufficient visibility of the programme to discharge their personal accountability. Internal audit must have a defined role in providing independent assurance over the programme, and their findings must be integrated into the TPRM remediation cycle.

Consumer Duty: Insurance and Retail Firms
For FCA-regulated firms with retail customers, the Consumer Duty creates an additional integration point. Where third parties are involved in the delivery of outcomes to retail customers, including claims management outsourcers, payment processors, or digital platform providers, the firm must assure itself that the third-party arrangement does not create a risk of poor customer outcomes. The monitoring framework for these arrangements must include customer outcome metrics alongside operational and financial risk indicators. FourthLine's TPRM methodology for insurance clients addresses this Consumer Duty dimension explicitly.

PS26/2: Integration with Incident Management and Governance
The PS26/2 and PRA PS7/26 reporting obligations, effective 18 March 2027, require TPRM to be integrated with the firm's incident management framework in a way that most programmes have not yet achieved. The 24-hour initial reporting deadline for qualifying operational incidents means that the incident management process must be connected directly to the TPRM programme. When a supplier event triggers an incident classification review, the relevant information about the supplier's materiality, the services affected, and the IBS dependencies must be available immediately to the team making the reportability assessment. A siloed incident management process, where operational staff manage the incident without reference to the TPRM register, cannot meet this requirement.

The annual register submission obligation also requires a formal integration point between the TPRM programme and the firm's regulatory reporting governance. The submission is not a one-off project: it is a standing annual obligation that requires the register to be maintained at a standard suitable for regulatory submission throughout the year, not prepared retrospectively. The governance calendar must include the annual submission as a fixed milestone, with defined ownership, data validation steps, and sign-off from the SMF24 holder before submission.

FourthLine's programme approach designs both integration points from the outset, rather than treating them as downstream additions to a core TPRM programme. The incident escalation process is designed to function as a regulatory reporting trigger as well as an internal management tool. The register maintenance process is designed to produce submission-quality data continuously, not just at year end.

The most common question FourthLine receives from COOs and risk leaders at the start of a TPRM conversation is not about what the regulation requires. It is about where they stand against it. Most mid-tier firms have some TPRM infrastructure, some documentation, and some process. What they do not have is an objective, evidence-based assessment of whether that infrastructure meets the regulatory standard, and where the most significant gaps lie.

That is precisely what FourthLine's TPRM Diagnostic is designed to provide.

What the Diagnostic Covers

The FourthLine TPRM Diagnostic is a structured review of the firm's current third-party risk management programme against the requirements of PRA SS2/21, FCA SYSC 8.1, FCA SYSC 15A, and, where relevant, DORA. It covers the full framework architecture: strategy, policy, supplier register, materiality methodology, due diligence approach, contractual standards, ongoing monitoring, exit planning, testing, and governance integration.

The Diagnostic is not a documentation review. It combines review of programme documents with structured interviews with the individuals responsible for running the programme across first-line business functions, the second-line risk and compliance function, and, where appropriate, the internal audit function. This gives a realistic assessment of whether the programme is operating as documented, not just whether the documentation exists.

What the Diagnostic Produces

The Diagnostic produces a structured gap register, a regulatory benchmark scorecard, and a prioritised action plan. The gap register maps specific findings against the relevant regulatory provisions and categorises each finding by severity: critical, where there is a clear regulatory breach or supervisory risk; high, where the programme does not meet the standard but the gap can be remediated within a defined timeframe; and medium or low, where improvement is needed but the risk is contained.

The action plan is not a list of recommendations. It is a sequenced programme of work that the firm can take directly into a TPRM improvement programme, whether that is delivered with FourthLine's support or internally. It addresses what needs to be done, why, in what order, and to what evidential standard.

When to Conduct a Diagnostic

A Diagnostic is appropriate at any of the following points: when a firm has a forthcoming supervisory engagement and needs to understand its current risk exposure; when a new SMF24 holder is appointed and needs an independent view of their inherited programme; when the firm has received regulatory feedback identifying TPRM weaknesses; when a material acquisition, outsourcing change, or corporate restructure has created new third-party risk that has not been assessed; or when the firm has built a TPRM programme but has not independently tested whether it meets the regulatory standard.

The publication of PS26/2 and PRA PS7/26 in March 2026, with an effective date of 18 March 2027, is itself a specific trigger. Firms that have not yet assessed their readiness for the pre-contractual notification requirement, the annual register submission, and the incident reporting calibration should commission a Diagnostic without delay. The twelve-month implementation window is tight for firms whose TPRM programme has structural gaps, and firms that begin preparations in the second half of 2026 will face a compressed delivery timeline.

Typical Engagement

A FourthLine TPRM Diagnostic typically takes two to four weeks from mobilisation to report delivery. It requires access to existing programme documentation, participation from the SMF24 holder and the first-line risk owners responsible for material supplier relationships, and engagement from the second-line risk or compliance function. The output is delivered as a structured written report with an accompanying presentation to the SMF24 holder and, where appropriate, the risk committee.

From Diagnostic to Programme

Most Diagnostic engagements transition into a programme of remediation work. FourthLine structures this transition to be efficient: the gap register and action plan produced by the Diagnostic become the programme initiation document, and the firm avoids the cost and delay of a separate scoping exercise. Where a firm has a defined timeline, such as a supervisory engagement or a self-assessment deadline, FourthLine designs the remediation programme to meet that timeline with appropriate prioritisation.

FourthLine: Who We Are and What We Deliver

Concentration risk: DORA Article 29 requires an explicit entity-level assessment before entering into arrangements supporting critical or important functions. UK frameworks address concentration risk but without the same pre-engagement assessment obligation.

Mandatory transition periods: DORA requires that contracts include a mandatory adequate transition period. PRA SS2/21 requires testing for feasibility but does not mandate a specific contractual transition period.

ICT third-party testing: DORA Article 25 explicitly includes ICT third-party systems in the testing scope. UK frameworks address this through the operational resilience testing cycle but without equivalent specificity.

Direct oversight: The DORA oversight framework for critical ICT providers creates a regulatory dimension with no direct UK equivalent. Firms must monitor designations and respond to oversight findings affecting their suppliers.