What we've learnt from working with building societies through to global banks

Third party risk: What to prioritise before March 2027

Guiding you through change with clarity and care

Advise. Assure. Deliver. Operational risk for building societies and banks



How much of your oversight changes a decision?

Start with what matters

We wrote this paper to help building societies and banks decide which supplier gaps to tackle first and how to prepare their people for March 2027.

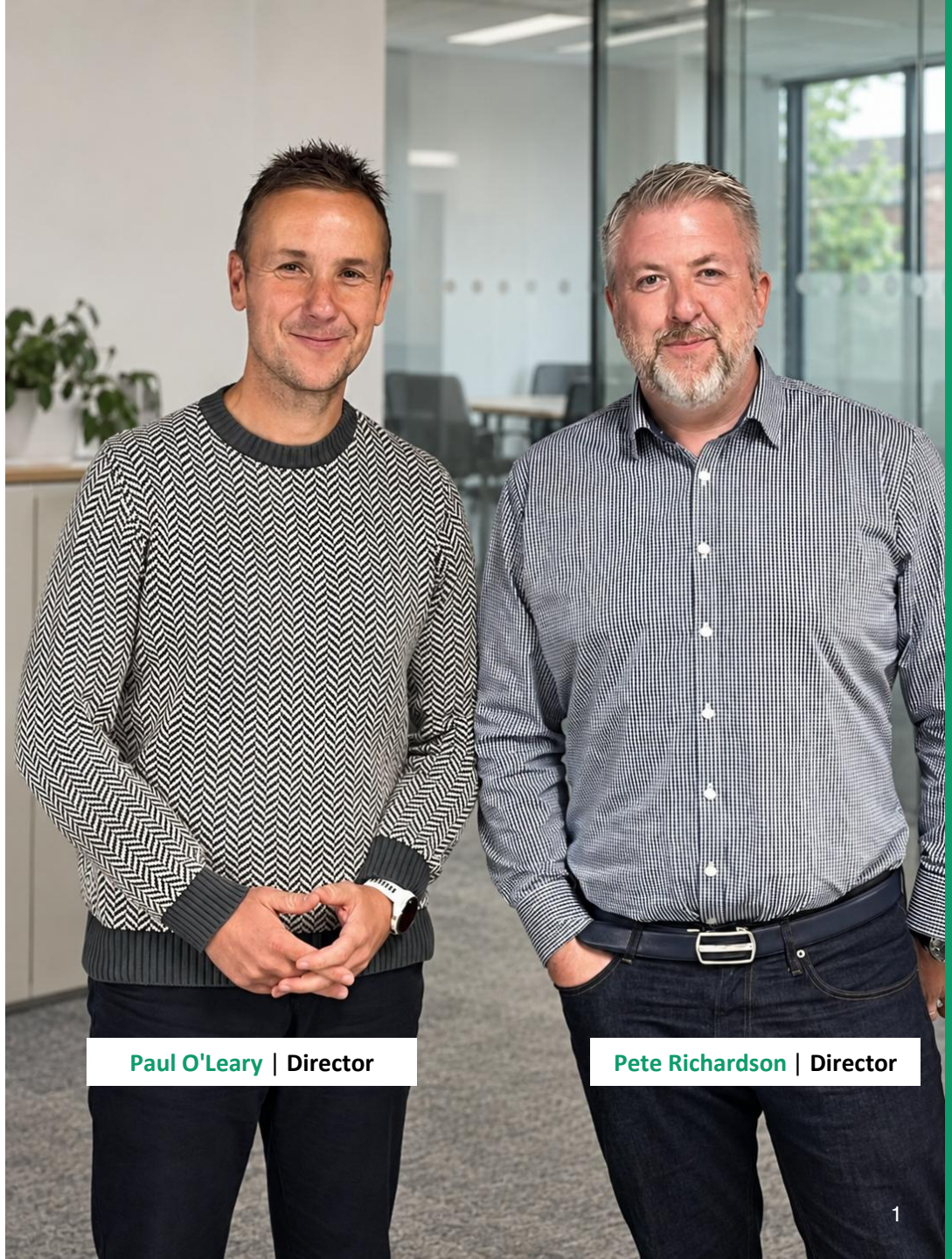
Our experience, from smaller building societies to global banks, has shaped our starting point: the approach must fit your firm's people, supplier relationships and existing systems.

That means finding gaps, challenging duplication and reducing unnecessary administration. Evidence can be reused where it covers more than one arrangement, and related supplier questions can be brought together. We know that constrained budgets, mean you need to get this right first time. This gives colleagues more time to investigate issues, apply judgement and work with the people needed to resolve them.

In our work, we've helped firms establish interim safeguards while pursuing lasting fixes. We've supported those responsible in bringing together colleagues across the business, with clear actions, owners and timescales. This gives leadership a clearer view of what has improved, what remains exposed and where decisions or support are needed.

In the pages that follow, we share the choices we would make in situations your team may face, the reasoning behind them and practical ways to put those ideas into use.

Our test is straightforward: does this paper help your team make a better decision and act on it?



Paul O'Leary | Director

Pete Richardson | Director

Green Dolphin

What is coming and why?



Our view:

Regulators want to understand shared supplier dependencies, see how firms manage the risks and respond quickly when disruption occurs. It is not expected to end disruptions.

If a supplier failed tomorrow, could your team establish the impact and make the reporting decision?

From **18 March 2027**, UK banks and building societies must use enhanced reporting for qualifying operational incidents. They submit an initial report, update it when circumstances change significantly, including when the incident is resolved, and complete a final report after resolution.

Separately, firms must notify regulators of planned new or significantly changed material third-party arrangements and submit an annual register.

Firms have **90 calendar days** from the FCA opening the register submission window. The **2027 return** reflects the position at **31 December 2026**.

At least **803**

hours of unplanned technology and systems outages across nine banks and building societies, January 2023 - February 2025.

NOW - DEC 2026

Over **40%**

of cyber incidents reported to the FCA in 2025 involved a third party.

Google

experienced a London-region cloud outage on 20 October 2026 which affected customer at banks and other organisations.

Fig 1: Evidence of operational disruption and supplier dependence

Green Dolphin

Why is this so hard to do?



Our view:

For most firms, the immediate priority extends beyond simply preparing a template submission. These activities represent an opportunity to enhance operational resilience, improve risk management, and gain strategic insights into your third-party ecosystem, rather than just meeting a compliance deadline.

Prioritise today's exposure and the time needed for a lasting fix. Build on existing resources wherever they meet the need.

The new requirements can expose existing gaps in **responsibilities, processes and information**, or change the priority of planned improvements. Closing those gaps may require coordinated changes across contracts, systems and teams. If the change required is significant, it needs change management support to be effective.

Information is fragmented

Contracts, variations, service reports and assurance evidence may be held by different teams - or by the supplier. Recovering and reconciling them takes time.

A missing document also needs investigating before concluding that the underlying safeguard is absent.

Ownership needs support

Improving an arrangement may require procurement, legal, technology, operations and risk colleagues to act, alongside the supplier.

Clear ownership needs supporting authority, information and capacity.

Dependencies extend further

A supplier may rely on cloud, telecommunications or other providers with whom you have no contract. Visibility and influence can be limited.

The challenge is establishing which dependencies matter and what relevant assurance is available.

Different gaps need different action

Missing records, weak contract terms and untested responses need different action. Match the response to the exposure, with interim protection where needed while longer-term fixes progress.

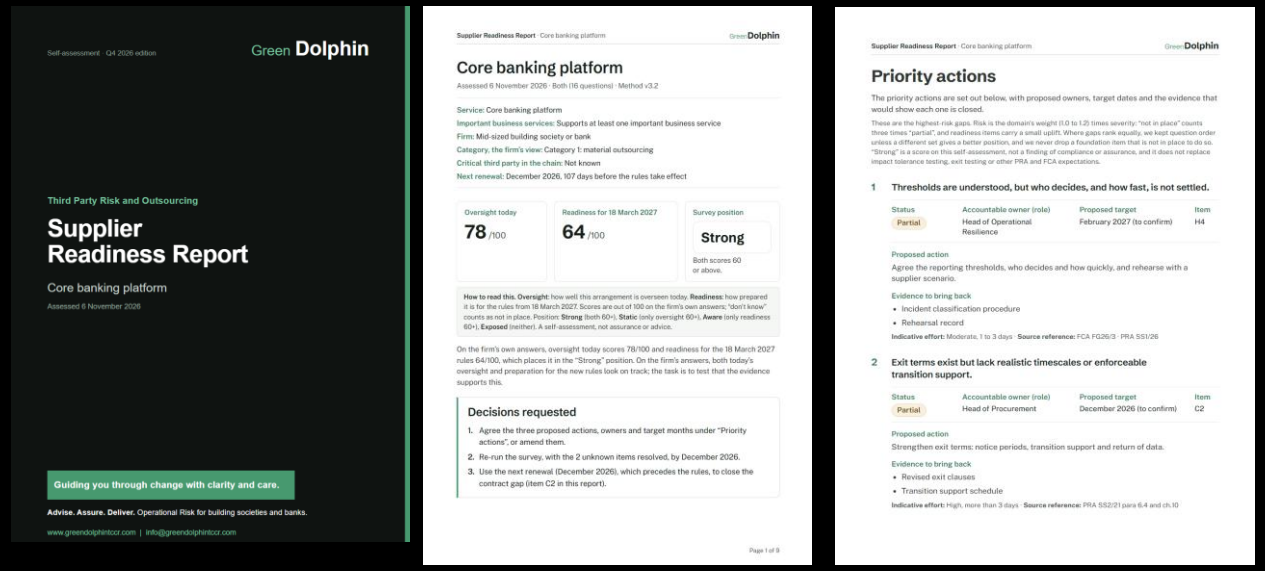
Apply checks according to risk, rather than treating every arrangement alike.

Fig 2: Key challenges on the road ahead to 18 March 2027

Start with a material supplier

Understand your oversight today and where preparation for March 2027 needs attention.

Our **free Supplier Readiness Self Assessment Tool** uses your answers to highlight potential gaps in one material supplier arrangement. Use the report to agree what to investigate, improve or test next: Supplier Readiness Report



Green Dolphin

Self-assessment · Q4 2026 edition

Third Party Risk and Outsourcing

Supplier Readiness Report

Core banking platform

Assessed 6 November 2026

Guiding you through change with clarity and care.

Advise. Assure. Deliver. Operational Risk for building societies and banks.

www.greendolphintcor.com | info@greendolphintcor.com

Supplier Readiness Report · Core banking platform — Green Dolphin

Core banking platform

Assessed 6 November 2026 · Both (16 questions) · Method v3.2

Service: Core banking platform
Important business services: Supports at least one important business service
Firm: Mid-sized building society or bank
Category, the firm's view: Category 1: material outsourcing
Critical third party in the chain: Not known
Next renewal: December 2026, 107 days before the rules take effect

Oversight today	Readiness for 18 March 2027	Survey position
78 /100	64 /100	Strong
		Both scores 60 or above.

How to read this. Oversight: how well this arrangement is overseen today. **Readiness:** how prepared it is for the rules from 18 March 2027. Scores are out of 100 on the firm's own answers; "don't know" counts as not in place. Position: **Strong** (both 60+), **Static** (only oversight 60+), **Aware** (only readiness 60+), **Exposed** (neither). A self-assessment, not assurance or advice.

On the firm's own answers, oversight today scores 78/100 and readiness for the 18 March 2027 rules 64/100, which places it in the "Strong" position. On the firm's answers, both today's oversight and preparation for the new rules look on track; the task is to test that the evidence supports this.

Decisions requested

1. Agree the three proposed actions, owners and target months under "Priority actions", or amend them.
2. Re-run the survey, with the 2 unknown items resolved, by December 2026.
3. Use the next renewal (December 2026), which precedes the rules, to close the contract gap (item C2 in this report).

Page 1 of 9

Supplier Readiness Report · Core banking platform — Green Dolphin

Priority actions

The priority actions are set out below, with proposed owners, target dates and the evidence that would show each one is closed.

These are the highest-risk gaps. Risk is the domain's weight (1.0 to 1.2) times severity: "not in place" counts three times "partial", and readiness items carry a small uplift. Where gaps rank equally, we kept question order unless a different set gives a better position, and we never drop a foundation item that is not in place to do so. "Strong" is a score on this self-assessment, not a finding of compliance or assurance, and it does not replace impact tolerance testing, exit testing or other PRA and FCA expectations.

1 Thresholds are understood, but who decides, and how fast, is not settled.

Status	Accountable owner (role)	Proposed target	Item
Partial	Head of Operational Resilience	February 2027 (to confirm)	H4

Proposed action
Agree the reporting thresholds, who decides and how quickly, and rehearse with a supplier scenario.

Evidence to bring back
- Incident classification procedure
- Rehearsal record

Indicative effort: Moderate, 1 to 3 days · Source reference: FCA FG26/3 · PRA SS1/26

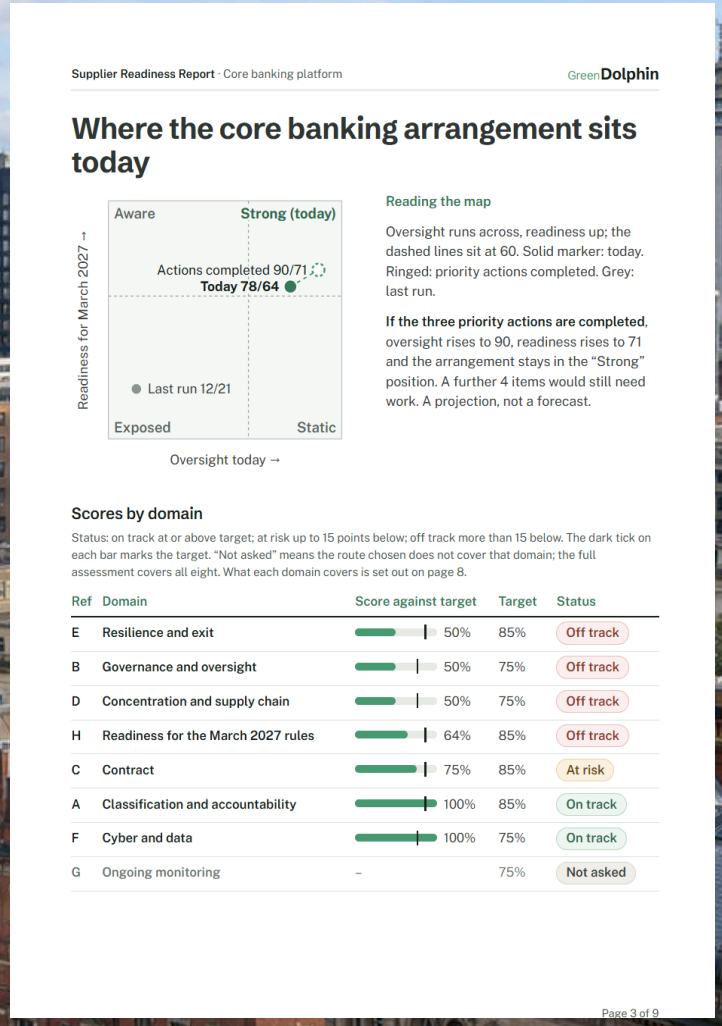
2 Exit terms exist but lack realistic timescales or enforceable transition support.

Status	Accountable owner (role)	Proposed target	Item
Partial	Head of Procurement	December 2026 (to confirm)	C2

Proposed action
Strengthen exit terms: notice periods, transition support and return of data.

Evidence to bring back
- Revised exit clauses
- Transition support schedule

Indicative effort: High, more than 3 days · Source reference: PRA SS2/21 para 6.4 and ch.10



Supplier Readiness Report · Core banking platform — GreenDolphin

Where the core banking arrangement sits today

Reading the map

Oversight runs across, readiness up; the dashed lines sit at 60. Solid marker: today. Ringed: priority actions completed. Grey: last run.

If the three priority actions are completed, oversight rises to 90, readiness rises to 71 and the arrangement stays in the "Strong" position. A further 4 items would still need work. A projection, not a forecast.

Scores by domain

Status: on track at or above target; at risk up to 15 points below; off track more than 15 below. The dark tick on each bar marks the target. "Not asked" means the route chosen does not cover that domain; the full assessment covers all eight. What each domain covers is set out on page 8.

Ref	Domain	Score against target	Target	Status
E	Resilience and exit	50%	85%	Off track
B	Governance and oversight	50%	75%	Off track
D	Concentration and supply chain	50%	75%	Off track
H	Readiness for the March 2027 rules	64%	85%	Off track
C	Contract	75%	85%	At risk
A	Classification and accountability	100%	85%	On track
F	Cyber and data	100%	75%	On track
G	Ongoing monitoring	–	75%	Not asked

Page 3 of 9

Fig 3: Material Third Party Supplier Readiness Report

Common pitfalls to avoid



Our view:

Start with what already works. Direct additional effort towards risk prioritised gaps that could leave you exposed.

Well-intended responses can add work and leave risks unresolved.

New questionnaires, tools and roles can help, but they need time and support to become effective and embed. If your firm is remediating existing gaps in third party management practices and implementing new systems, meeting the new requirements may mean the plan will need to be rephased. Establish what is missing, what existing arrangements already provide and who needs to act. Choose a response your firm can operate and sustain.

The same checks for every supplier arrangement 01

Match assessment and oversight to the arrangement's risk and materiality. Record the rationale for a lighter approach.

Accepting assurance without checking what it covers 02

Check what the evidence covers and excludes, whether it is current, and its relevance to the service you use.

A new tool before a clear need 03

Define the information gap first. Check whether existing systems and assurance can meet the need before buying or building more - what's within your risk appetite and what's not.

Contract work left until renewal 04

Review terms early. Where a gap matters now, consider interim protection while pursuing a lasting fix.

Giving responsibility without the support to deliver 05

Agree who will deliver each change and ensure they have the authority, expertise and capacity to act.

Testing only with complete information 06

Test whether your team can make reporting decisions and submit required reports on time with incomplete supplier information. Record assumptions, information gaps and what remains untested.

Fig 4: Common pitfalls summary

Green Dolphin

Difficult choices to make

We'd prioritise gaps that leave you exposed today, start longer-term fixes early, and focus on changes that strengthen multiple arrangements, with any residual risk remaining transparent, governed and agreed.

A possible situation	How we'd respond
The register will be ready in March, but not December	**Preserve the 31 December 2026 position and keep later fixes distinct.** We'd validate for the notified window and use short sessions with supplier owners to resolve unreliable entries.
We can't find every material arrangement contract	**Start where uncertain rights create the greatest exposure.** We'd recover complete terms, distinguish missing paperwork from missing protection and start urgent changes before renewal.
Should quarterly scenario testing cover multiple suppliers?	**Not automatically. Target assurance gaps first.** We'd use short focused testing exercises for decisions; test recovery where needed and widen coverage when justified. Leave time to fix and retest and ensure you can stand behind the approach taken. Could you outsource your testing to provide the capacity, speed of delivery and knowledge transfer you need?
The supplier never agreed to provide this data	**Agree interim reporting now. Keep the contract gap visible.** We'd agree what the supplier sends, to whom and when. Then we'd test whether those updates support a reporting decision and escalate any shortfall.
The supplier has not mapped its fourth parties	**Start with dependencies that could stop the service or its fallback.** We'd compare providers, hosting locations and recovery arrangements to see where the same dependency could affect several services or take out both the main service and its fallback. Ask suppliers for evidence on the gaps that matter and record what remains unknown. A simple map can be enough, with specialist tools worth considering where dependencies are harder to trace.
Third party management and incident reporting are separate processes	**This does not require a single team. It requires connected people and processes.** This isn't a new topic, so we'd recommend you build on existing processes, adapting incident definitions, triage criteria and escalation triggers to align with the new requirements and reporting thresholds.

Fig 5: How Pete and Paul would handle these situations

Green Dolphin

Preparing for 18 March 2027

Six practical steps towards third-party and incident reporting readiness.

These activities overlap. **You should start changes involving suppliers, contracts or systems early, and test processes as they develop.** Your reporting arrangements should be working, with people prepared to use them, by 18 March 2027. For the 2027 register return, this should report the position as of 31 December 2026.

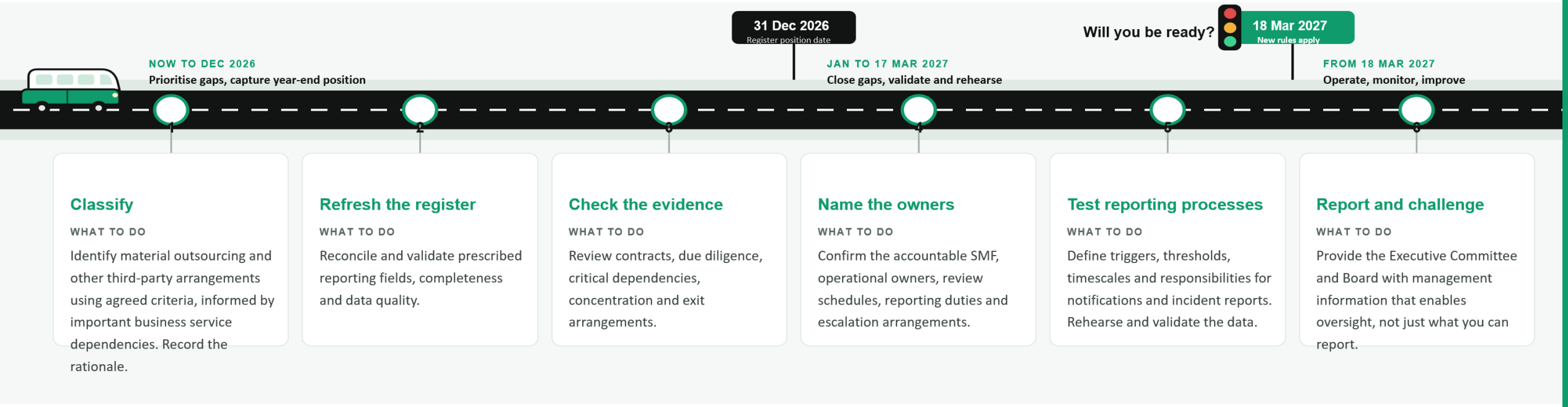


Fig 6: Outline actions and roadmap

Green Dolphin

Know you're ready for March and beyond

Use your gap analysis to decide what to fix and test first.

Bring together the changes that apply to your firm and the gaps you already know need fixing. For each significant gap, ask what the fix depends on and whether leaving it open could make a return inaccurate, delay a notification or leave the team without enough information to make an incident reporting decision. Start with one material third-party arrangement, then widen testing to cover different teams, systems and suppliers.

Show leadership what worked in testing, what still needs fixing and retesting before March, and where a decision or support is needed.

01 Year-end return

Can we stand behind the register?

Trace sampled entries to year-end evidence. Reconcile the register, then validate and rehearse uploading the full return.

From 31 December 2026

Check that changes are captured. Reconcile the register before each return.

02 A proposed hosting move

Would we know whether to notify?

A supplier proposes moving member data to a new hosting region. Assess whether the move materially changes the risks. If it does, rehearse submitting the notification before the firm commits, including who would step in if the usual submitter is away.

From 18 March 2027

Sample the actual decisions and check that the required notifications were sent in time.

03 A Friday 4pm outage

Could we act on an incomplete update?

Ask the supplier's incident contact for an update through the usual channel. Assess the impact, decide whether to report and rehearse the submission.

From 18 March 2027

Use actual incidents and exercises to continually find delays, prioritise improvements and retest fixes.

Fig 7: Tests that will provide confidence

Give yourself time to prepare

Early visibility into new regulation and emerging sector issues gives you time to assess the impact, plan changes that take longer and build on arrangements already in place.

As your firm relies more on AI tools provided through material third-party arrangements, it's important to know which services depend on those tools and what would happen if a supplier could no longer provide them.

Our free Operational Risk Radar brings together regulatory developments, sector lessons and our judgement on what deserves attention. It gives you questions to raise and evidence to request, helping you spot developments early and build proportionate action into existing plans. Explore the Operational Risk Radar.

We focus on the evidence, the implications and the practical response.

Green Dolphin

> **Where sufficient assurance cannot be obtained firms should strengthen their own contingency arrangements.**
>
> Andrew Bailey and Nikhil Rathi in their joint response to the Treasury Committee (4 November 2026)
>
> Ref: Critical Third Parties regime and Google Cloud service disruptions

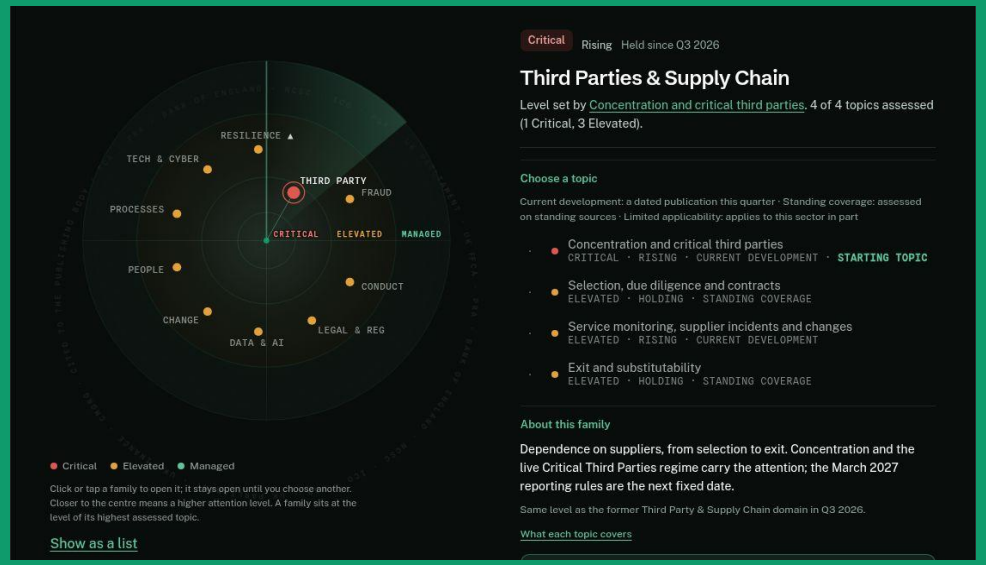


Fig 8: Green Dolphin Risk Radar

Green Dolphin



Pete Richardson | **Director**

Pete@greendolphintccr.com

Know what matters. Act now.

- Start with one material third-party arrangement. Establish what you can rely on, what needs protection now and what will take longer to fix.
- Bring the right colleagues into the work. Reuse suitable evidence and rehearse decisions involving several arrangements, including when supplier information is incomplete or remediation is still under way.
- Give leadership a clear account of what is fixed, what remains exposed and what needs a decision.
- When information is incomplete and time is short, your people need clear responsibilities and arrangements they can use.

Talk to Pete or Paul about your arrangements or your next reporting exercise.



Paul O'Leary | **Director**

Paul@greendolphintccr.com

YouTube

How we can help

Challenge

The same colleagues were keeping services running, supporting a transformation and assessing suppliers. With no dedicated third-party risk manager, they shared the work alongside their day jobs. New suppliers needed timely decisions while existing assessments were still waiting. The bank needed a way to manage supplier risk that its team could sustain.

Approach

We started with how the team already worked. We assessed the gaps, clarified who was responsible for what, and updated the policy and procedures. We cleared the assessment backlog and ran joint pilots on live supplier assessments, linking supplier oversight to incident management, operational resilience, and regulatory and Board reporting.

Outcome

- **Pace of change:** The bank kept new supplier decisions moving in support of its growth plans.
- **Confidence:** Business owners became more confident running assessments and brought Risk in earlier, giving teams and suppliers more time to gather evidence.
- **Proportionate support:** The bank handled routine assessments in-house and drew on specialist advice for more complex arrangements.
- **Stronger assurance:** A follow-up audit assessed the remediated controls more favourably.
- **Back within appetite:** KPIs returned to target and KRIs moved back within agreed thresholds.

Fig 9: Bank case study (unsecured loans, credit cards, insurance and savings)



Green Dolphin

Green **Dolphin**

Values

Do what is right

Better our communities

Bias for action

Always human

Embrace difference

What we believe

Our mission is to give every building society and smaller bank the senior expertise they need to navigate change, manage risk, and serve their members well, without the cost, complexity, or compromise that comes with working with a large firm.

Twenty per cent of our profits go back into the communities our clients serve (see examples: Click)

Guiding you through change with clarity and care

www.greendolphintccr.com | info@greendolphintccr.com

YouTube

The contents herein remain the intellectual property of Green Dolphin (TCCR) Limited, registered in England and Wales. They may not be reproduced, shared, or relied upon without prior written consent. Company Number: 16855006.

“Highly likely to recommend to another CEO or Executive”



Based on engagements delivered between 1 January to 30 September 2026