THE PRA'S OUTSOURCING AND THIRD-PARTY RISK MANAGEMENT GUIDELINES:

Everything you need to know to prepare for changes ahead

ProcessUnity

PROCESSUNITY WHITE PAPER

CONTENTS

EXECUTIVE SUMMARY:
THE CHANGING FACE OF RISK IN THE FINANCIAL SERVICES INDUSTRY

What could cause systemically important financial services firms to fail and put the global economy at risk?

In the aftermath of Lehman Brothers' collapse, regulators put huge amounts of time and effort into answering this question, and made sweeping reforms aimed at ensuring events like the 2008 financial crisis never happened again.

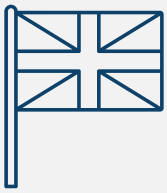
But while governance, conduct, and operational controls are important, rapid digitalisation throughout the 2010s, and events like the Brexit referendum, and, more recently, the Covid-19 pandemic have shown it's not just firms' culture and appetite for risk that could bring them down.

In an interconnected world, the outsourcing arrangements regulated firms are increasingly reliant on could cause just as much damage if third party suppliers don't meet required standards.

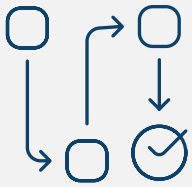
Against this backdrop, the Prudential Regulatory Authority, a United Kingdom financial services regulatory body that supervises 1,500 financial institutions, has issued new guidelines that explain how regulated firms should outsource business-critical functions and manage the associated risks.

In this white paper, we'll look at:

Why the Prudential Regulatory Authority has issued these guidelines



How the guidelines will change outsourcing and third-party risk management in the UK



What key steps in-scope firms should start taking today to prepare ahead of the 31 March 2022 implementation deadline

THE EVOLUTION OF OUTSOURCING

Banks, financial services firms, and, indeed, businesses in most other industries have been outsourcing in some shape or form since at least the early 1980s. But the role outsourcing plays in businesses' wider strategies has changed dramatically since the turn of the millennium.

When firms first started outsourcing, they usually did so to reduce costs. Farming out non-core activities — payroll, or legal services such as litigation, for instance — saved time and money, and allowed them to focus on their core business competencies.

As their comfort level with outsourcing grew, firms realised the practice had other compelling benefits, and their approach evolved.

First, they started farming out activities that directly impacted business performance, because it helped them gain valuable outside perspectives and be more competitive.

But the biggest transformation came about during the latter half of the 00s and the start of the 2010s.

With rapid digitalisation and a constantly shifting, increasingly complex and competitive landscape, doing everything in-house became unsustainable. As a result, firms started outsourcing business-critical functions, including regulated activities, to strategic partners.

According to a recent survey, **86% of Tier 1 investment banks** outsource between two to four core functions to third-party providers, with the other **14%** outsourcing four or more.

Similarly, **17% of Tier 2 and Tier 3 investment banks** outsource at least one core function, with **50% outsourcing two to four,** and **33% outsourcing more than four.**

These arrangements have allowed firms to be more flexible, agile, and adaptable. But they've also created new risks for customers and the financial system as a whole.

As the Basel Committee on Banking Supervision, the International Organisation of Securities Commissions, and the International Association of Insurance Supervisors noted in a remarkably forward-looking 2005 joint report:

'Outsourcing has the potential to transfer risk, management, and compliance to third parties who may not be regulated, and who may operate offshore. In these situations, how can financial services businesses remain confident that they remain in charge of their own business and in control of their business risks? How do they know they are complying with their regulatory responsibilities? How can these businesses demonstrate that they are doing so when regulators ask?'

A global financial crisis, a momentous political decision, and a deadly pandemic later — the Brexit referendum and Covid-19 pandemic have both increased demand for and the complexity of outsourcing arrangements — these questions have never been more pertinent.

And that's where the Prudential Regulatory Authority's Outsourcing and third-party risk management guidelines come in.

BRINGING OUTSOURCING INTO THE 21ST CENTURY

The Prudential Regulatory Authority's Outsourcing and third-party risk management guidelines, which will come into force on 31 March 2022, have two main objectives.

First, they provide much-needed clarity around a number of long-standing regulatory requirements firms must follow when outsourcing.

Second, and more to the point, they aim to develop the rules on outsourcing, bringing them in line with the latest technological developments and modern practises.

The guidelines closely mirror those published by the European Banking Authority in February 2019 (though they differ in a number of subtle ways), and apply to the following PRA-regulated firms:

- Banks
- Building societies
- Credit unions
- Insurers and reinsurers
- Investment firms that meet the following criteria:
  - » Have permission to deal with investments as principals
  - » Have a minimum capital of €730,000 (around £623,500) or are broadly similar to an EEA passporting firm
  - » Meet the criteria of a designated investment firm
- UK branches of third-country banks and insurers

That said, third-party service providers should familiarise themselves with the guidelines too, even if they're unregulated. Their PRA-regulated clients will need to make sure the relationship is compliant.

It's also worth noting that, while the official deadline is 31 March 2022, this is for new outsourcing arrangements only. Firms must review any arrangements they currently have in place at the 'first appropriate contractual renewal or revision point.'

Needless to say, if the first appropriate renewal or revision point is before 31 March 2022, that's when the arrangement must become compliant.

THE PRA GUIDELINES IN PRACTICE: HOW WILL OUTSOURCING CHANGE?

The PRA's guidelines address six key areas of the current rules on outsourcing:

01. The definition of outsourcing

02. The threshold for materiality, that is the point at which an outsourced function becomes so important its weakness or failure would put the firm in breach of the PRA's fundamental rules

03. Proportionality

04. Concentration risk

05. Terms an outsourcing contract must include

06. Notification requirements

Let's take an in-depth look at the changes in each area.

Defining Outsourcing

The guidelines adopt the definition of outsourcing in the PRA rulebook:

'...an arrangement of any form between a customer and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be undertaken by the customer itself.'

That said, they make two important clarifications.

Firstly, firms must consider whether the third party will perform the service as a one-off, or on a recurring or ongoing basis.

Secondly, and more significantly, they make it clear that buying the following products or services generally isn't outsourcing (though it may be in some circumstances):

- Hardware, software, and other tech products, including the design and build of on-premises platforms
- 'Off the shelf' machine learning models, including training models and data libraries
- Insurance aggregators and delegated underwriting

Similarly, saving data to the cloud isn't necessarily outsourcing.

The PRA recognises that third parties are ultimately responsible for the integrity of cloud infrastructure such as servers. That said, firms should make sure they manage and store data in a way that's compliant and take steps to prevent security breaches.

Assessing Materiality

The guidelines set out seven criteria firms have to consider when assessing materiality:

01. Whether there's a direct connection to the performance of a regulated activity

02. The size and complexity of the relevant business area or function

03. The potential impact on business continuity, operational resilience, operational risk, or the firm's ability to comply with its legal and regulatory requirements

04. The impact on customers and counterparties

05. The potential impact on recovery and resolution plans

06. The firm's ability to scale up the outsourced services

07. How easy it is to replace the service provider or bring the function back in-house

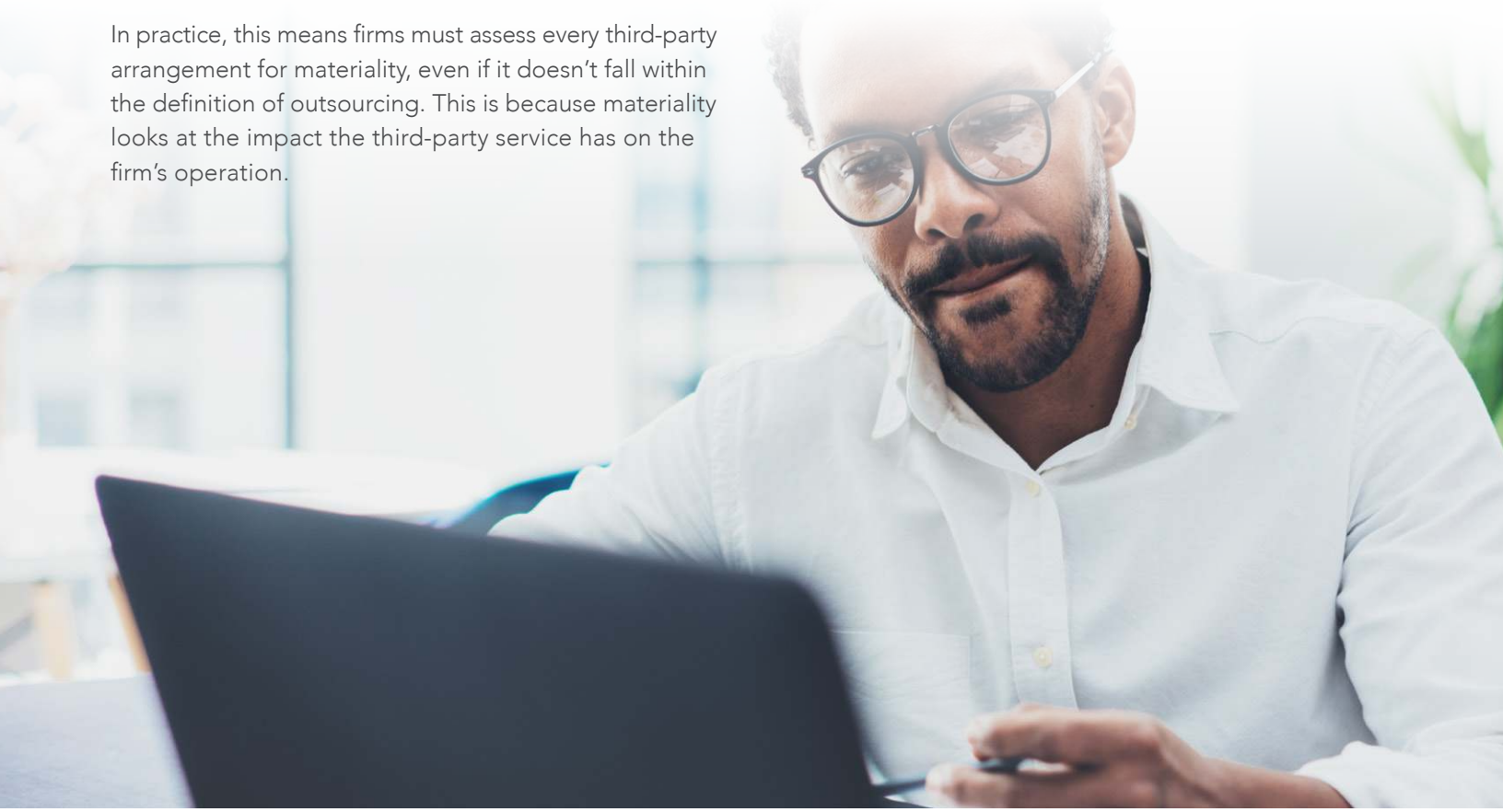
In practice, this means firms must assess every third-party arrangement for materiality, even if it doesn't fall within the definition of outsourcing. This is because materiality looks at the impact the third-party service has on the firm's operation.

Spreading Risk

The guidelines make it clear that firms must take reasonable steps to manage concentration risk and lock-in risk — the risk of becoming too reliant on a single supplier.

Concentration risk and lock-in risk arise when there are:

- Multiple arrangements with the same provider, or with a number of providers that are connected to each other
- Fourth-party or supply chain dependencies. In other words, the providers, though not connected, depend on the same sub-contractor
- Arrangements that are difficult or impossible to substitute
- Several arrangements in the same geographical area, even if the suppliers aren't connected to each other



Getting the Details Right

Outsourcing agreements for material functions should have a number of specific provisions. These include:

- A clear description of the outsourced function, as well as any support services
- The start date, next renewal date, end date, and any notice periods. The guidelines also specify a number of circumstances under which a firm should have a right to end the agreement
- The agreement's governing law
- Financial obligations
- Whether the supplier can sub-outsource, under which terms, and when the firm can reject sub-outsourcing
- The location where the service will be provided, plus an obligation to let the firm know if this is going to change
- Provisions on data accessibility, availability, integrity, confidentiality, privacy, and safety
- A right to monitor the service provider's performance on an ongoing basis, including inspecting and auditing them when necessary
- A service level agreement, including business continuity arrangements.

There's an obligation to tell the PRA if a third-party service provider is unable or unwilling to include certain terms in the contract — though it's unclear what consequences (if any) firms will face for failure to do so.

That said, the PRA's guidance is more flexible and less prescriptive than the EBA guidelines when it comes to the actual text of the agreement.

The Proportionality Principle

Proportionality — the principle that rules should apply in a manner that is appropriate to a firm's size and the nature of their activities — is well-established in UK financial services regulation. So it's no surprise that it also applies under the PRA's guidelines.

While all firms that are within the guidelines' scope must comply, a small firm's obligations are less onerous than those of a systemically important bank.

Notifying the PRA

The guidelines specify two instances when firms have to notify the PRA:

- If any 'critical or important' arrangements entered into on or after 31 March 2021 aren't compliant by the deadline
- In advance, whenever firms enter or 'significantly change' a material outsourcing arrangement

Crucially, the PRA will consider whether they've been notified on time when evaluating compliance with fundamental rule seven — the requirement to deal openly and cooperatively with the regulator.

...the PRA's guidance is more flexible and less prescriptive than the EBA guidelines...

PREPARING FOR THE DEADLINE: 4 STEPS TO HELP YOU GET COMPLIANT BY 31 MARCH 2022

While, on paper, 31 March 2022 is a hard deadline, the reality is that — as with every new regulatory initiative — there's going to be a ramping up period after which the PRA will assess how firms are meeting the requirements.

While no one can anticipate how aggressively the PRA will enforce the requirements, it is widely believed that it's going to be taken very seriously — which is why it's fundamental to start preparing sooner, rather than later.

Here are four steps firms should start taking today to make sure they're ready by the deadline.

1.

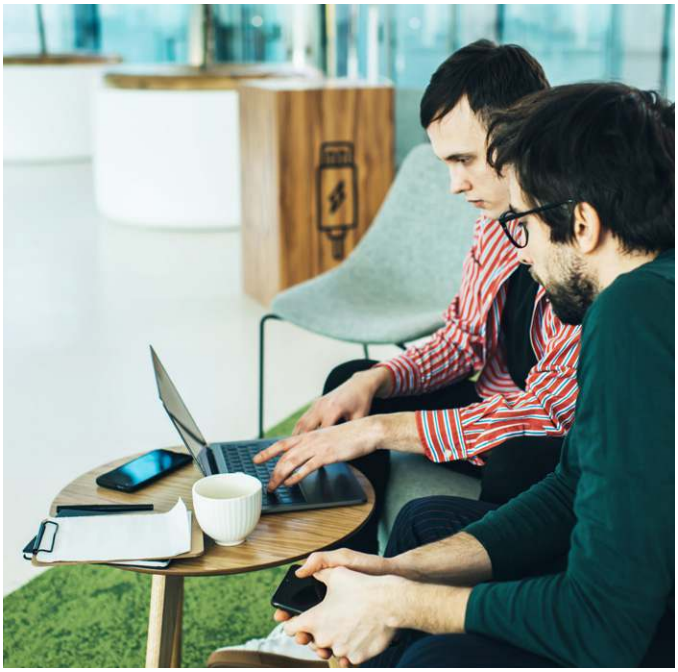
DEVELOP AN APPROPRIATE METHODOLOGY FOR ASSESSING MATERIALITY

Assessing materiality is the cornerstone of the guidelines.

The PRA has laid down very specific criteria firms must consider when making the assessment. Being able to understand and interpret them is important.

What's even more critical, though, is developing a clear, repeatable, and auditable framework that works at scale.

The PRA's guidelines will come into play every time firms put in place new arrangements or alter existing ones. Having this framework will speed things up and help make sure nothing falls through the cracks.



2.

UNDERSTAND OUTSOURCING RISKS AND TAKE STEPS TO MINIMISE THEM

The whole point of the guidance is to make sure firms don't leave their customers unsupported if a third-party service provider is unwilling or unable to continue supplying business-critical services.

This means firms must:

- Have a strong understanding of the risks involved when outsourcing a particular function. In other words, what could possibly go wrong?
- Take steps to minimise those risks

Hitting both of these aims requires a two-fold approach.

Needless to say, carrying out proper due diligence is a must:

- Does the supplier have a disaster recovery plan in place? What does it look like?
- Do they have the right level of information security controls?
- And what other measures do they have in place that ensure they can continue providing their services safely and uninterruptedly?

But this is only one piece of the puzzle. While functions can be outsourced, responsibility and accountability can't. With this in mind, it's crucial to exercise proper oversight, including by using access, audit, and information rights to make sure suppliers are fulfilling their obligations on an ongoing basis.

3.

PUT ROBUST CONTINGENCY PLANS IN PLACE

Things can go wrong despite the most thorough due diligence and everyone's best intentions. That's why firms should have documented and tested business continuity plans and exit strategies in place.

The guidelines require firms to have two exit strategies:

- **A stressed exit,** where the third-party can't continue supplying the service because of issues such as a major data breach or a critical infrastructure failure
- **A non-stressed exit,** where the contract ends due to commercial or strategic reasons, disagreements, or because the firm is unhappy with the third party's level of service

A robust business continuity plan should set out in detail how the outsourced service will be returned in-house in stressed and non-stressed scenarios. Or, alternatively, there should be a fall-back service provider that can take over while keeping service interruption to a minimum.

4.

PUTTING TECHNOLOGY TO WORK

If the amount of work that needs to be done — both in preparation for the 31 March 2022 deadline and on an ongoing basis — feels overwhelming, that's because there's a lot of ground to cover.

The good news is that there are technologies that have packaged best practises into a reliable, repeatable, and automated process, so firms can prepare and stay compliant with less effort.

ProcessUnity Vendor Risk Management is a centralised platform that enables you to handle every step of the outsourcing process — from pre-contractual selection and due diligence to ongoing monitoring, performance assessments, and contract management — from one convenient, user-friendly location.

With ProcessUnity Vendor Risk Management, firms can:

Simplify vendor sourcing and selection

Put standardised sourcing procedures in place and create, distribute, and evaluate questionnaires, requests for information, and requests for proposal.

Our sourcing module automatically scores responses based on custom criteria and makes it easy to compare suppliers or conduct more in-depth analysis.

Conduct comprehensive due diligence

Create probing, insightful questions and evaluate responses using pre-set parameters in line with internal policies.

Our platform also carries out automatic risk assessments and categorises suppliers accordingly, including identifying any relationships that might create concentration risk or lock-in risk under the PRA guidelines.

Easily manage outsourcing contracts

Create PRA-compliant contract templates in just a few clicks and effortlessly keep track of their status, including the dates when they're due for review or due to expire.

Monitor third-party service providers

Our software can handle every aspect of supplier monitoring, including:

- Documenting service level agreements and keeping track of whether suppliers are meeting expectations
- Designing PRA-compliant procedures and tests for on-site assessments
- Identifying and documenting any issues and tracking progress towards resolving them

About ProcessUnity

ProcessUnity is the leading provider of cloud-based risk management and compliance software. The world's top organisations trust us to help them identify, manage, and mitigate their third-party and information security risks.

About DVV Solutions

We are an authorised ProcessUnity Managed Service Partner (MSP). Our managed services and solutions are proven to improve your ability to assess, analyse and manage more third-party risk domains, utilising the full power of ProcessUnity's Vendor Risk Management platform.

Want to learn more about how DVV Solutions and ProcessUnity can help your organisation prepare for the PRA guidelines?

Schedule a demo today - Click Here.

ProcessUnity

www.processunity.com
info@processunity.com
978.451.7655
Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States

DVV solutions

www.dvvs.co.uk
enquiries@dvvs.co.uk
+44.0.161.476.8700
Twitter: @dvvs_tprm
LinkedIn: dvv-solutions

DVV Solutions
Grosvenor House
Stockport, SK1 3TZ
United Kingdom