UK FINANCE

PRA SS2/21
THE COMPLIANCE JOURNEY

In association with:

CAPCO
a wipro company

Authors and contributors

Ian Burgess
Director, Cyber and Third Party Risk, Payments & Innovation, UK Finance

Zelfau Rauof
Analyst, Cyber and Third Party Risk, UK Finance

Gatikrushna Mishra
Managing Principal, Capco

Nicole Wright
Consultant, Capco

UK Finance

UK Finance is the collective voice for the Banking and finance industry. Representing more than 300 firms, UK Finance acts to enhance competitiveness, support customers and facilitate innovation.

Contacts
Information on UK Finance can be found at:
www.ukfinance.org.uk
Please contact Data and Research for payment market information:
ukfstatistics@ukfinance.org.uk
Please contact Corporate Affairs for press queries or general information:
info@ukfinance.org.uk
For information about membership of UK Finance, please contact:
membership@ukfinance.org.uk

Capco

Capco, a Wipro company, is a global technology and management consultancy specialising in driving digital transformation in the financial services industry. With a growing client portfolio comprising over 100 global organisations, Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent. To learn more, visit **www.capco.com** or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

Third Party Risk Management (TPRM) has been and will continue to be an increasing area of focus for the financial industry, with growing regulatory focus on efforts to strengthen third-party resilience at industry level.

One of the most significant TPRM regulations for the UK financial industry is the Prudential Regulatory Authority's (PRA) Third Party and Outsourcing (SS2/21) Supervisory Statement (SS). It was published on 29 March 2021 with a compliance date set to 31 March 2022 and outlines a comprehensive set of resilience expectations for the industry. It was published in conjunction with new standards (SS1/21) for Operational Resilience, with the intent to embed SS2/21 as one of the core pillars for Operational Resilience.

Impacted financial institutions (FIs) experienced varying levels of challenges on their journey to compliance. Although some tactical means were adopted to cross the finish line by 31 March 2022, a front to back review and upliftment of the existing TPRM operating model became evident in order to maintain compliance. Another interesting but not surprising observation was the importance of better collaboration amongst all participants in the TPRM ecosystem – a) service providers, b) recipient FIs and c) regulators.

This paper has four sections:

1. **Section 1:** Overview of SS2/21 requirements
2. **Section 2:** Impact on the financial industry
3. **Section 3:** The journey to compliance
4. **Section 4:** Key considerations for FIs

SECTION 1: OVERVIEW OF SS2/21 REQUIREMENTS

In the last decade, the financial industry has significantly scaled up its reliance on third parties, primarily driven by the fast-paced adoption of cloud computing services, and the emergence of fintechs. The TPRM regulatory landscape has consequently gained momentum to support this growing pace and to ensure industry level resiliency.

The PRA SS2/21 requirements are comprised of several key themes (as shown in Figure 1).

Figure 1. SS2/21 Themes

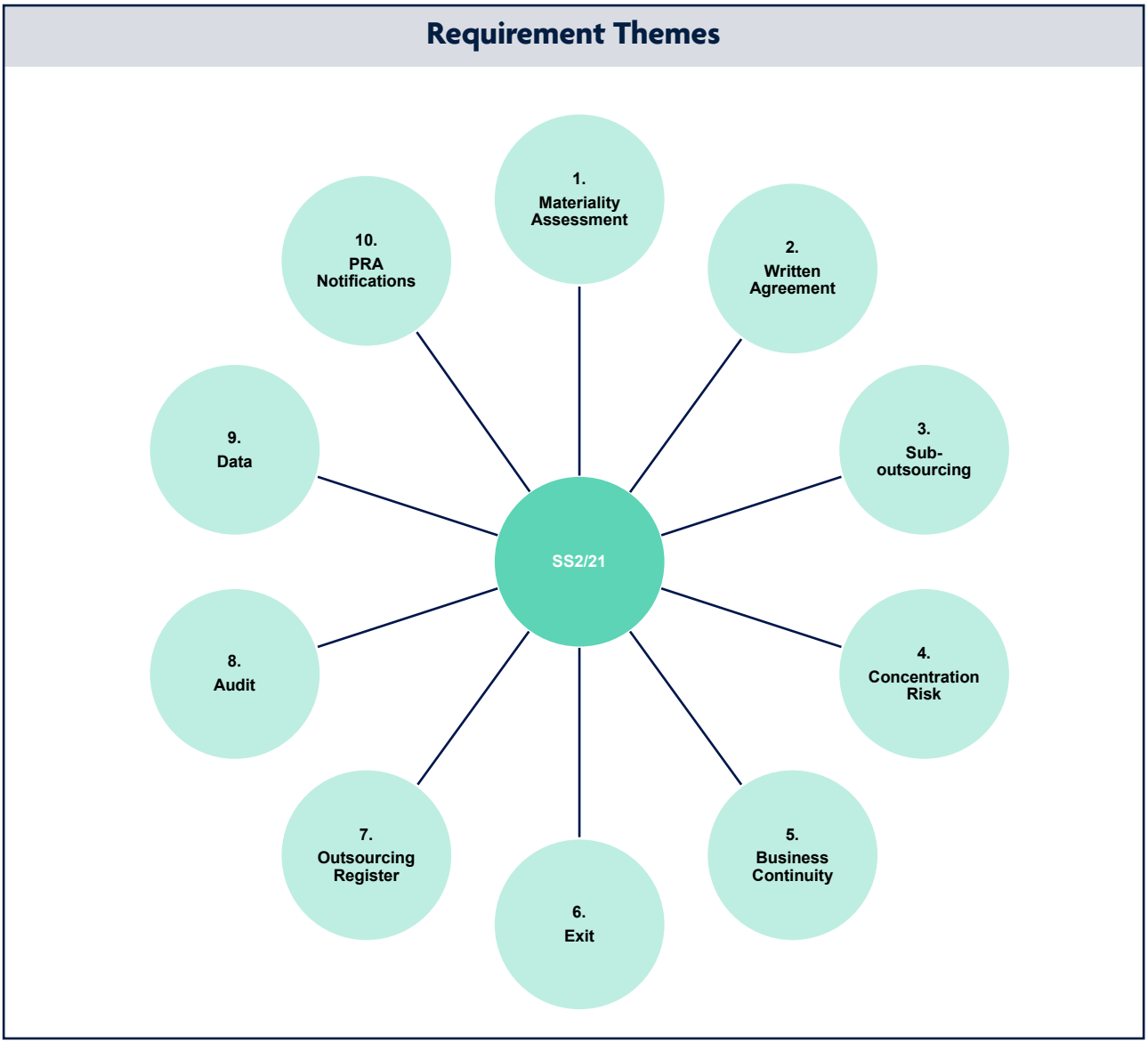


Table 1. SS2/21 Themes and requirement summary

THEME	REQUIREMENT SUMMARY
Materiality Assessment	Assess materiality for all third-party arrangements, based on specific criteria, prior to commencement of service.
Written Agreement	Written agreements for material services must include specific provisions, including information and audit access rights.
Sub-outsourcing	Identify and manage complex subcontractor chains.
Concentration Risk	Identify and manage concentration risk.
Business Continuity Plan (BCP)	Develop, implement, maintain and test BCPs for material arrangements with the ability to deliver important business services (IBS) in line with impact tolerances in the event of disruption.
Exit	Document and maintain an exit strategy to provide a last resort risk mitigation strategy in the event of disruption that cannot be managed through other business continuity measures. The exit strategy must cover planned and stressed exit scenarios.
Outsourcing Register	Maintain a register of outsourced arrangements.
Audit	Exercise audit rights (as required) including consideration for onsite audits.
Data	Manage data risks for material arrangements.
PRA Notification	Notify the PRA Supervisory Team when 1) arrangements are deemed as material, 2) service provider unable or unwilling to contractually facilitate a firm's compliance with regulatory obligations 3) alternate means to assurance is considered.

SECTION 2: IMPACT ON THE FINANCIAL INDUSTRY

The PRA SS2/21 publication came in the midst of the ongoing implementation of the EU's EBA Guidelines for Outsourcing (EBA GL) which enabled FIs to leverage their preparation for EBA compliance to support SS2/21 compliance, while acknowledging the key differences between both regulations. The most striking differentiator in SS2/21 is the paradigm shift of focus from outsourcing (in EBA GL) as a key driver for due diligence to materiality (in SS2/21).

With the SS2/21 compliance date set to 31 March 2022, three months after the EBA GL compliance deadline (31 December 2021), certain UK FIs had to balance focus and effort concurrently on the implementation of both regulatory requirements.

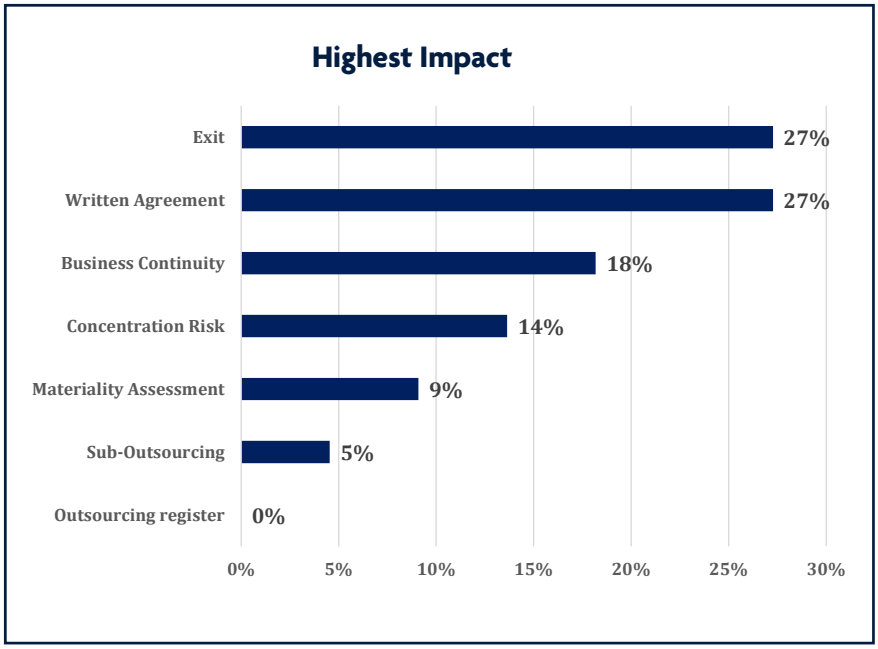
UK Finance and Capco conducted a survey of UK Finance's members in July 2021. The primary objectives of the survey were to 1) identify the SS2/21 themes which had the highest impact on compliance efforts and overall resilience, and 2) understand the compliance maturity of members at the start of their SS2/21 compliance journey.

JULY 2021 SURVEY INSIGHTS

The survey included seven of the ten themes. A total of 22 members responded to the survey, ranging from fintechs and building societies to large universal banks.

Themes with highest impact

Figure 2. Survey Findings: Themes with highest impact

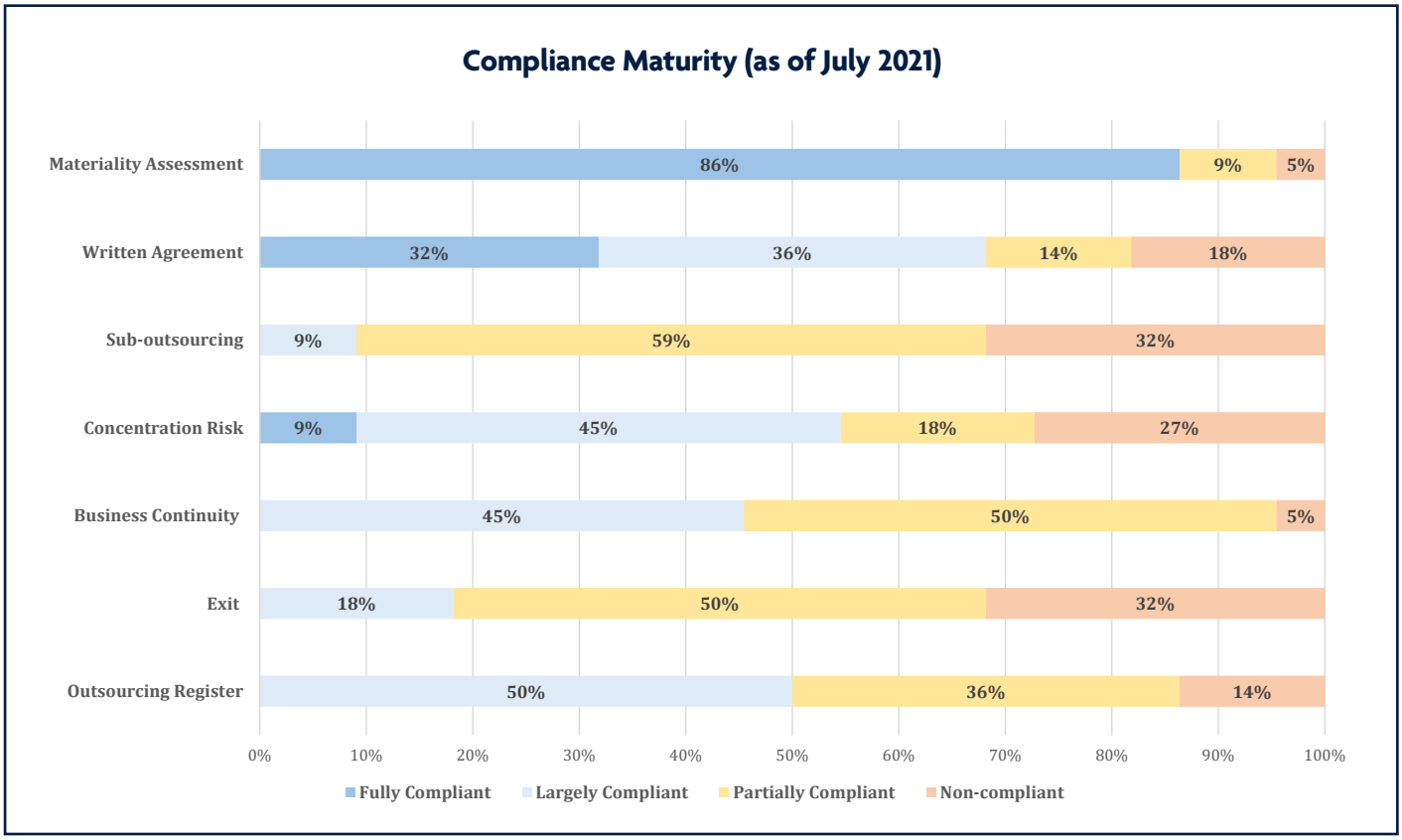


- **Exit Strategy** and **Written Agreement** emerged as the top two themes with the highest impact, as per 54% of the survey respondents.
- **Business Continuity** and **Concentration Risk** emerged as the next pair of themes with highest impact, as per 32% of the survey respondents.

Compliance maturity per theme

Figure 3. highlights the compliance maturity of members, against four levels (see footnote on page 6), as of July 2021.

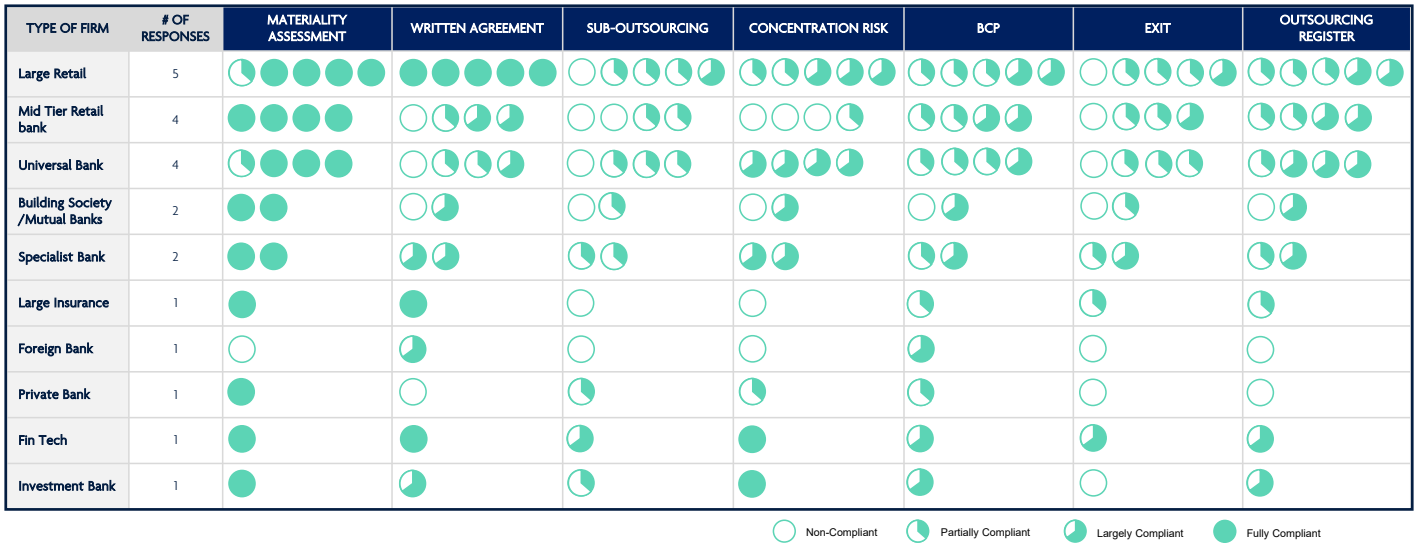
Figure 3. Compliance Maturity Summary (as of July 2021)



- Exit Strategy and Sub-outsourcing were the themes with the least compliance maturity amongst members. **32%** of members were non-compliant with both themes, and at least another **50%** partially compliant.
- Concentration Risk, Written Agreement and Outsourcing Register were the next set of themes with lower compliance maturity.
- Materiality Assessment was the only theme with the most significant amount of compliance maturity.

Compliance maturity by member groups per theme

Figure 4. Compliance Maturity per theme (as of July 2021)



1. Fully Compliant: Members already have processes in place for the themes as highlighted and meet all the requirements.
2. Largely Compliant: Members have processes in place which meets most of the requirements but not all.
3. Partially Compliant: Members have processes in place which meet some of the requirements but require significant changes to be compliant.
4. Non-Compliant: Members either do not have processes in place or existing process require complete overhaul to be compliant.

SECTION 3: THE JOURNEY TO COMPLIANCE

Analysis from the survey highlighted that some members were already focused on enhancing their operating model to comply with the EBA outsourcing requirements and were partially compliant in some of the identified themes. However, the need for additional improvements to the operating model was necessary for many of the members as identified through UK Finance member discussions.

The scope of compliance included meeting the minimum standard by 31 March 2022, for at least those engagements which were entered into a contract on or after 31 March 2021. In addition, where possible, legacy engagements should also be aligned to the SS2/21 requirements by 31 March 2022 or at the earliest review.

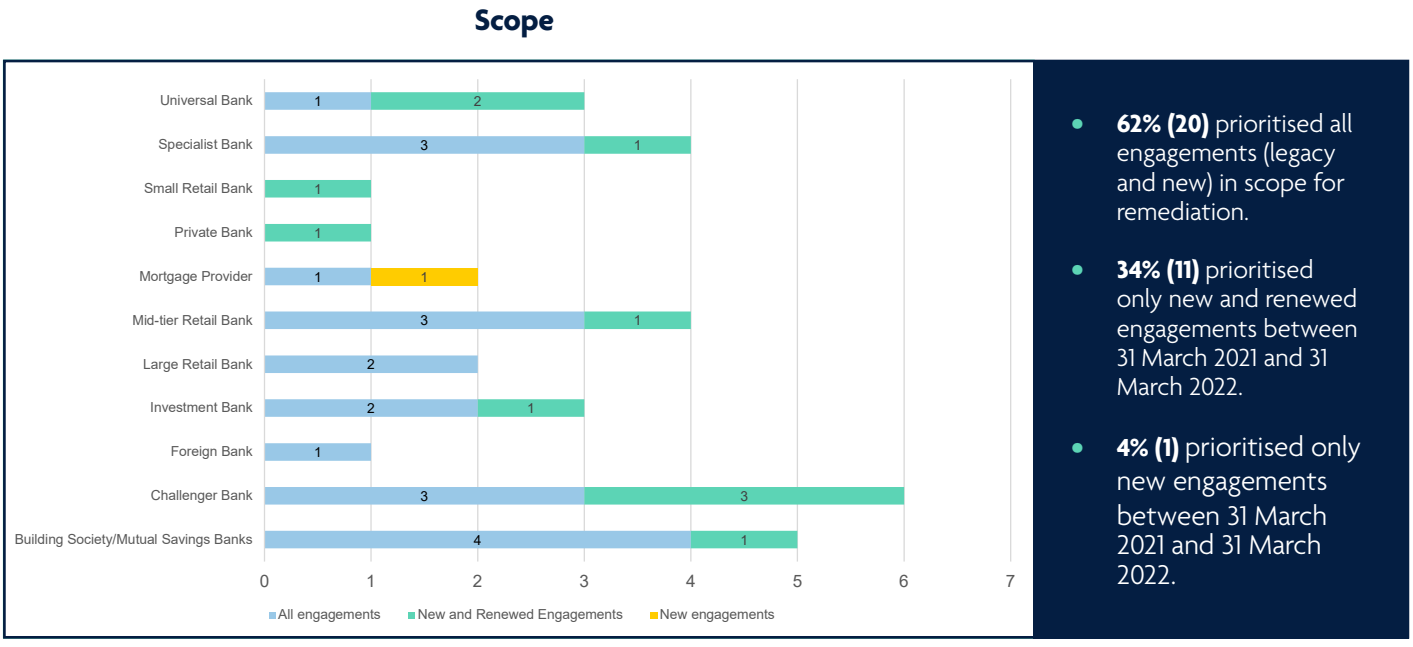
From the July 2021 survey (Figure 3.), it was evident that the journey to compliance still required considerable effort. UK Finance and Capco conducted specific deep dive sessions on key topics as agreed with members to better understand those issues.

March 2022 Survey insights

In Q1 2022 and ahead of the PRA's 31 March 2022 compliance deadline, UK Finance and Capco conducted a follow up survey (concluded in March 2022) to obtain a view of the progress in compliance maturity and readiness.

32 members responded to the survey. Figure 5 (below) summarises the scope of engagements for compliance for each category of member firms. The survey highlighted that most members prioritised all engagements both new ones entered into contract on or after 31 March 2021 and engagements which existed prior to 31 March 2021.

Figure 5. Scope of engagements for compliance by 31 March 2022

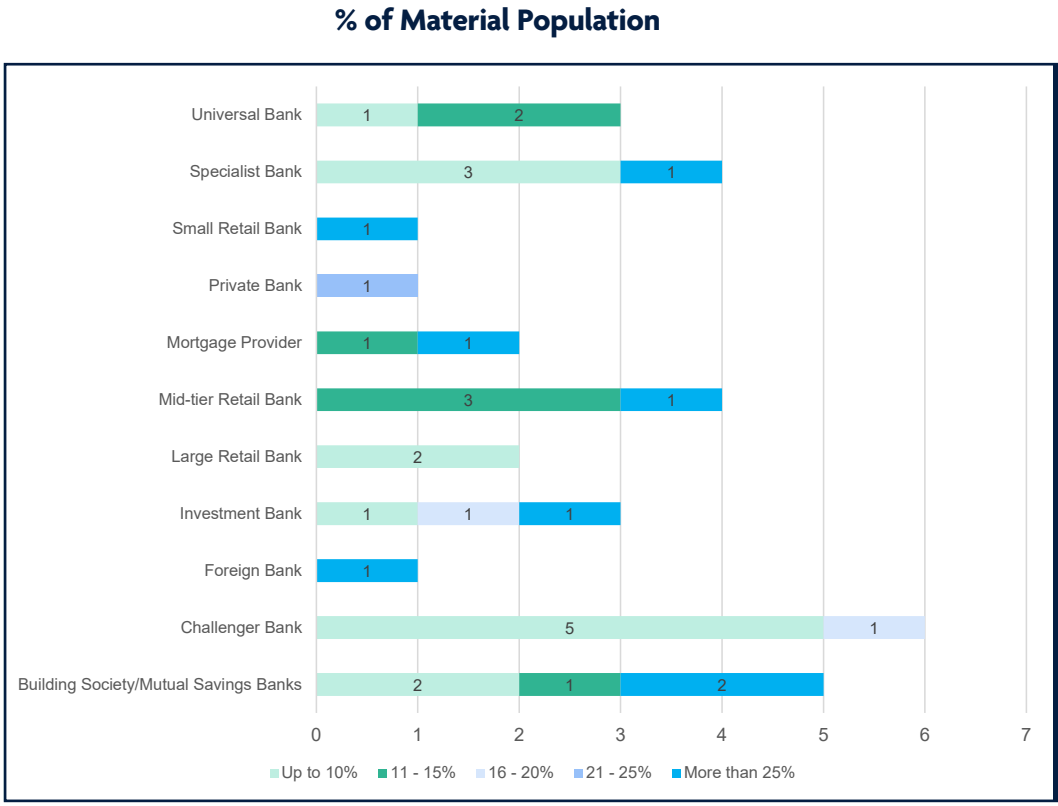


Materiality assessment

A materiality assessment for the engagements is a pivotal first step as it triggers the subsequent due diligence and as seen in the survey responses, the volume of engagements deemed as material and the maturity of the existing operating model informed the scale of effort required to meet compliance.

The March 2022 survey highlighted that most of the mid-tier and small firms had more than 25% of their total engagements as material, while large firms had less than 15% of their total engagements as material.

Figure 6. Volume of material engagements



- **44% (14)** have up to 10% of the third-party population as material and in scope.
- **22% (7)** have 11-15% of the third-party population as material and in scope.
- **6% (2)** have 16-20% of the third- party population as material and in scope.
- **3% (1)** have 21-25% of the third-party population as material and in scope.
- **25% (8)** have more than 25% of the third-party population is deemed material and in scope.

External dependencies

Another key factor to achieve compliance was the cooperation from external third-party providers. Prior to SS2/21, external providers were involved and aware of the regulatory requirements for outsourcing engagements. However, with the focus on materiality (for both outsourcing and non-outsourcing) in SS2/21, the volume of non-outsourcing service providers in scope for compliance significantly increased and achieving full compliance significantly relied on cooperation from external providers.

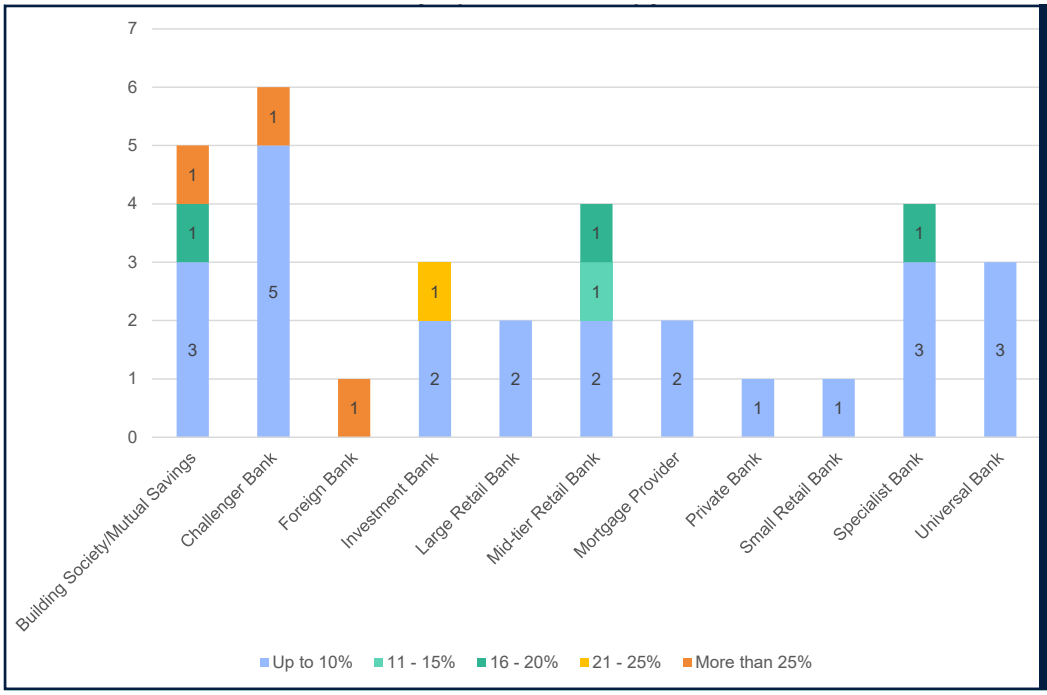
A drawback noted by members was that some of their larger service providers were inundated with requests for additional information within a stringent timeframe to support compliance readiness.

There were three key themes where reliance on external providers was inevitable:

1. **BCP**
   External providers to demonstrate resiliency in the material services they provide to an FI.
2. **Written Agreement**
   External providers to agree to additional contractual provisions, including information and audit rights, for material services.
3. **Sub outsourcing**
   External providers to demonstrate resiliency in their supply chain for the material services they provide to an FI.

Figure 7. Risk of non-compliance due to external provider dependency

% of External Third Party Expected To Not Comply with BCP & Contracts



- **75% (24)** of the members expected up to 10% of the external vendors to not comply with BCP and/or Contracts.
- **3% (1)** of the members expected between 11 – 15% of external vendors to not comply with BCP and/or Contracts.
- **9% (3)** of the members expected between 16 – 20% of external vendors to not comply with BCP and/or Contracts.
- **3% (1)** of the members expected between 21 – 25% of external vendors to not comply with BCP and/or Contracts.

Compliance readiness

Finally, it was time to understand the compliance readiness by 31 March 2022. The survey results for compliance readiness are highlighted in figures 8 and 9.

Figure 8. Compliance Readiness for 31 Mar 2022

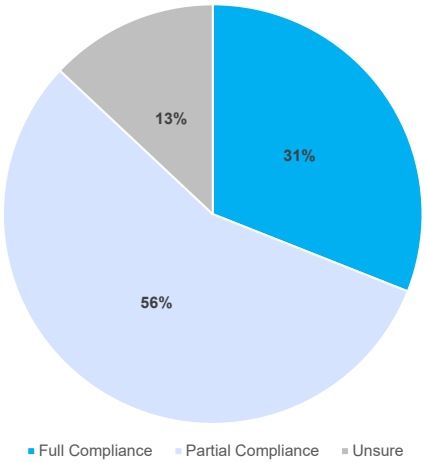
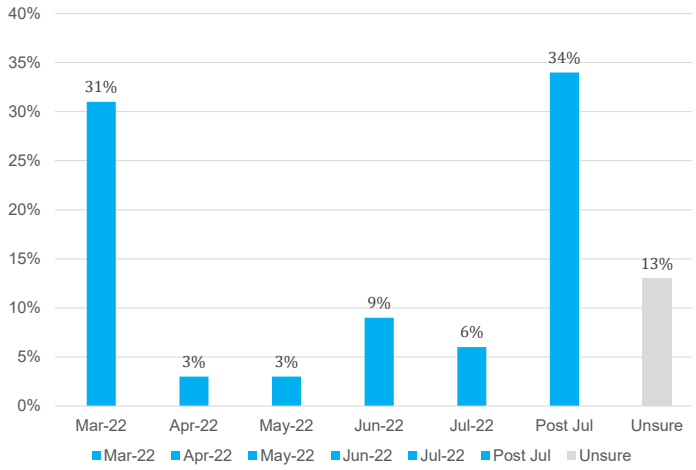


Figure 9. Compliance Readiness Timeframe



- **31% (10)** of the members were on track for full compliance by 31 March 2022.
- **56% (18)** of expected to be partially compliant by 31 March 2022, and fully compliant in Q2 and Q3 2022.

- **15%** of the members were on track to be partially compliant by 31 March 2022, and fully compliant by 30 June 2022
- **6%** of the members were on track to be fully compliant by July 2022
- **34%** of the members expected to be fully compliant post July 2022

SECTION 4: KEY CONSIDERATIONS FOR FIs

The third-party landscape and regulatory compliance requirements are constantly evolving, and at a fast pace. A list of key upcoming regulations is noted in Table 2.

Table 2. Key Regulations

- Critical Third Parties Regime (BoE/FCA/PRA/HMT)
- Outsourcing Register (PRA)
- Incident Reporting (PRA)
- Digital Operational Resilience Act aka DORA (EC)
- EU Data Act (EC)

These regulations will enable the regulators to gain further transparency of systemic concentration risk within the financial industry.

Compliance with regulatory requirements has been a primary driver for change within the financial industry and is likely to remain so. Compliance as a catalyst, not the end game, calls for firms to carefully consider a strategic risk and resilience-based approach to enhancing their existing operational environment to not simply meet compliance but for overall operational resilience.

Implementing a stategic approach will not be sustainable to keep up with the plethora of regulations as it can lead to an increase in the level of operational risks while diminishing the return on investments (ROI) within an organisation. The lack of prioritisation of operating model components such as strategic technology and data architecture, fit for purpose organisation models (skilled resources, training), standardised processes, analytical capability and governance may also hinder the maturity of an FIs TPRM maturity.

In addition to a strategic approach, the role of industry-level collaboration on third-party resilience is essential. It provides an opportunity for both industry and regulators to gain visibility of individual and sector wide third-party resilience while enabling ease in resilience assessment for both third-party providers and FS recipients. FIs, providers and regulators all play a pivotal role in the ecosystem (listed below).

Recipient FIs

- Prioritise strategic approach to manage third-party risks effectively.
- Consider a utility model to obtain standard information about providers centrally.
- Progress towards perpetual TPRM from periodic reviews (annual).

Providers

- Increase awareness about TPRM regulations and resiliency requirements.
- Implement robust supply chain resiliency for their supply chains.
- Collaborate with recipient FIs in strengthening resiliency including testing.

Regulators

- Harmonise resiliency requirements globally.
- Leverage existing regulations, if already meeting resiliency requirements, for key non-outsourcing providers.
- Address resiliency gaps in regulatory requirements for key non-outsourcing providers.

CONCLUSION

Third-party resilience is an important element for recipient FIs, regulators and providers.

It enables:

- the recipient FIs to be nimble in adapting to changing customer needs and optimising value to customers
- the regulators to manage systemic risks
- the providers to continue to provide services and support the compliance needs of recipient FIs

Therefore, it is prudent for each party to review and amend (as appropriate) existing operating models and increase the collaboration to drive industry level third party resiliency.

BIOS

Ian Burgess

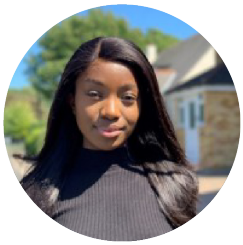
Ian leads UK Finance's operational and policy work on cybersecurity and third party risk management. In this role he leads responses to regulatory papers both in the UK and internationally, while also regularly engaging with key stakeholders to determine the applicability of collective action initiatives on behalf of the financial sector. Most notably he operationalised the Financial Sector Cyber Collaboration Centre (FSCCC), a unique industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Before joining UK Finance, Ian worked in technology risk at BNY Mellon, where he led the development and deployment of a global framework to map controls to global cyber, technology and data privacy regulations, and before that served an eight year career as a British Army Officer.

Gatikrushna Mishra

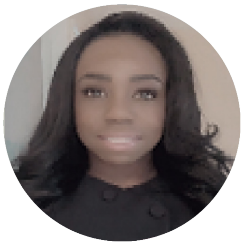
Gati is a Managing Principal at Capco and author of the PRA SS2/21 paper. He is the global head of Third-Party Risk Management (TPRM) and Procurement consulting practice. He has more than 20 years of experience in Transformation with more than 12 years of experience in Financial and Non-financial Risk Management.

Before joining Capco, Gati worked in Risk Advisory in EY where he led initiatives to review risk, control framework, and enable regulatory compliance such as FRTB, Stress Testing and ICAAP. Prior to EY, he worked in Tier 1 banks - Goldman Sachs, Morgan Stanley and JPM Chase.



Zelfau Rauof

In her role at UK Finance, Zelfau engages with key stakeholders across the sector on relevant cyber and third party policies to ensure the collective voice of the Financial Sector is maintained. She also provides secretariat support to the development of the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions. Prior to working at UK Finance, Zelfau worked as a Depositary Analyst within private equity.



Nicole Wright

Nicole is a Consultant at Capco London and a contributor to the PRA SS2/21 paper. She has Third-Party risk, SOX Compliance experience and 10+ years experience in research, analysis, strategy, change management and critical integration management. She has managed engagement portfolios in SOX across global business functions for a Tier 1 bank and responsible for delivery and operations for Systems and Organizational Controls reporting, process and efficiency improvements.