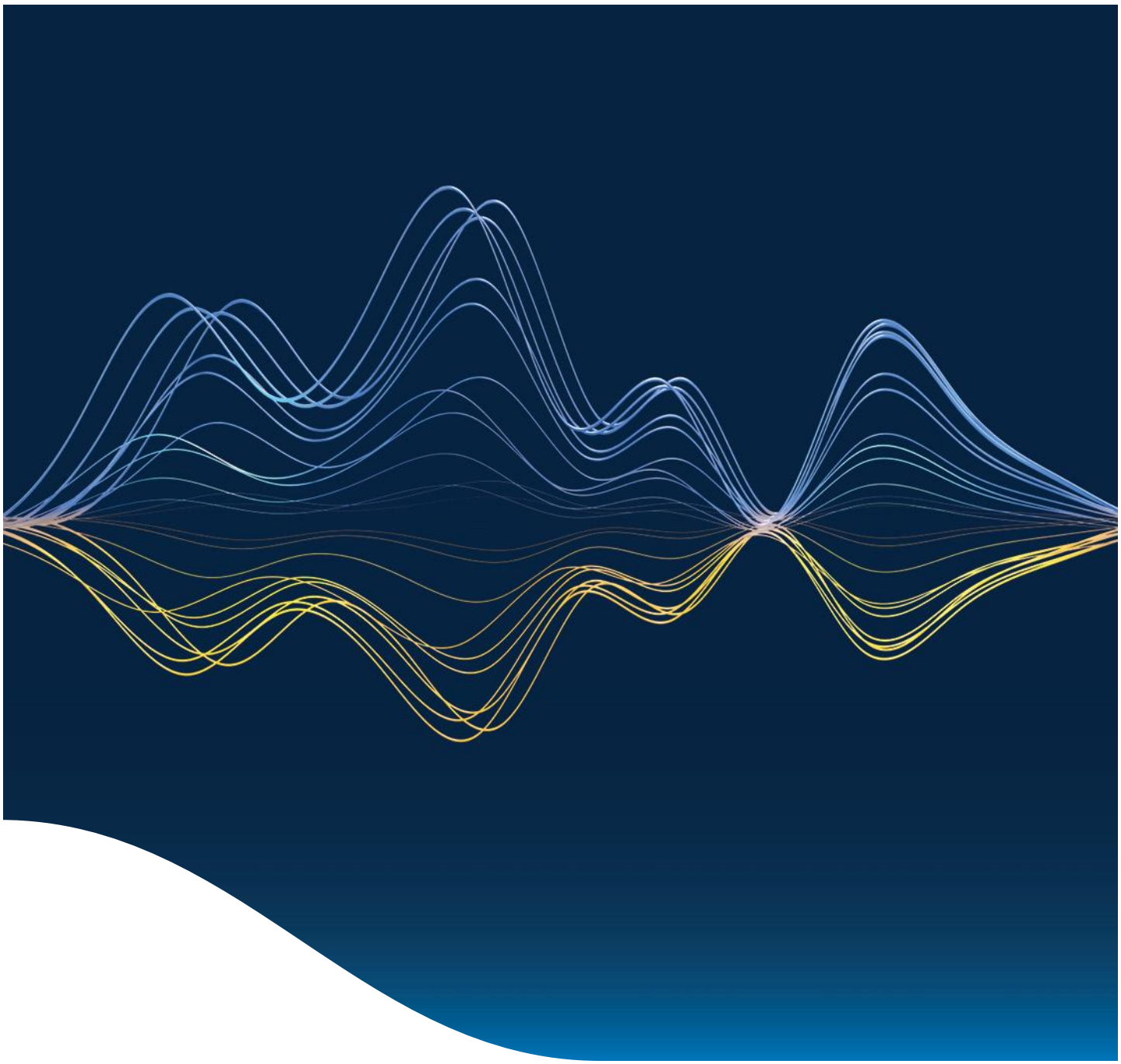

Outsourcing, Third Party Risk Management and Operational Resilience

The PRA's Supervisory Statements

DLA PIPER

March 2021

Outsourcing and Third Party Risk Management – the PRA's Supervisory Statements

After a period of anticipation, the PRA has now issued (on 29 March 2021) two linked policy statements and associated Supervisory Statements, namely:

a. Policy Statement (PS7/21) and Supervisory Statement (SS2/21) on Outsourcing and Third Party Risk Management; and

b. Policy Statement (PS6/21), Supervisory Statement (SS1/21) and PRA Rules on Operational Resilience: Impact Tolerances for Important Business.

These are the results of widespread consultation following the PRA's Consultation Paper 30/19 in December 2019, and look to consolidate the PRA's requirements regarding not just outsourcing arrangements but also other material service arrangements. Significantly, they will apply both to banks and insurers, and so help to create a more coherent and consistent regulatory landscape for financial services firms in the UK. They are also specifically geared to cope with the post Brexit landscape, and to enact those European requirements which will continue to be of relevance going forward (e.g. the EBA Guidelines on Outsourcing) whilst only "taking note" of those which will not (e.g. the EIOPA outsourcing guidelines and the ESMA guidelines on outsourcing to cloud service providers)….albeit that the PRA has stated that it anticipates that its requirements will be "at least equivalent" to those other European provisions.

Looking at Operational Resilience and Supervisory Statement SS1/21 first, the requirements will be effective as from 31 March 2022. Firms must have a plan for compliance which is put in effect before this date, but the PRA recognises that the "full extent of sophistication" of mapping and scenario testing may not be completely in place by then. It appears that there may then be a further period to make any necessary progress to get any issues identified and bring recovery times back within the identified impact tolerances; the long stop date for this set at 31 March 2025.

SS1/21 focusses upon "important business services" i.e. the services which, if disrupted, would impact the PRA's objectives and thereby the public interest (and which could pose a threat to the firm's safety or soundness or ultimately the financial stability of the UK). Policyholder protection is also a designated focus for insurers. The focus is accordingly away from individual systems, and towards continuity of services to end users. Specifically, it does not include internal services (such as HR) per se, i.e. on a standalone basis; the PRA is giving priority to those services which are outward facing. However, they say that if the internal services are part of the "chain" of activities which underpin an important business service, then they do need to be included in the firm's mapping, testing and remediation plans.

The key obligation is to identify all "severe but plausible" exposures in relation to the important business services, and to then set an "impact tolerance" in relation to each one, i.e. the maximum period or extent of disruption which would be bearable. Once these tolerances have been set, firms will need to put in place whatever measures are required in order to ensure that they will not be

breached in practice. This is clearly a substantial exercise and one which will need to be put in train at an early stage.

SS1/21 expressly cross refers to SS2/21 in terms of the need to include outsourcing arrangements within the risk mapping exercise, but SS2/21 itself goes further and looks to translate the EBA Guidelines on outsourcing into the UK regulatory regime. All outsourcing arrangements entered into on or after 31 March 2021 should comply with its requirements; legacy contracts are also to be reviewed and updated at "the first appropriate contractual renewal or revision point" so as to meet SS2/21 expectations "as soon as possible on or after 31 March 2022" (a welcome extension beyond the original December 2021 deadline envisaged by the EBA). Note therefore that legacy contracts might not need to be fully compliant as of 31 March 2022, come what may, which may be a relief to firms who are not as yet well advanced in their EBA remediation programmes.

On the flip side, however, PRA has stated that it expects firms to assess the materiality and risks of ALL third party arrangements, irrespective of whether they fall within the usual definition of "outsourcing" (i.e. so as to include other forms of services arrangements, such as system implementation projects for example). Where such arrangements are identified as being material or high risk, there should be "proportionate, risk based, suitable controls" which are as robust as those which would apply to an outsourcing agreement of equivalent materiality or risk. A critical non outsourcing agreement may therefore have MORE stringent requirements than a less critical outsourcing arrangement. This has implications for those firms who are already part way through their EBA remediation programmes, as they may now need to bring into scope contracts which are not considered to be "outsourcing" arrangements, but where they would be considered by the PRA to be material to the firm's operations. A good example would be a major IT/platform implementation project.

SS2/21 generally mirrors the approach and terminology used by the EBA Guidelines, and focusses upon "material" outsourcing projects, i.e. those services of such importance that weaknesses or failures in relation to them would cast serious doubt upon the firm's continued satisfaction of threshold conditions or compliance with the Fundamental Rules. The PRA has however clarified that this would also include services described elsewhere in EU legislation as "critical or important" functions.

SS2/21 also contains certain subtle but potentially important deviations from some of the detailed requirements of the EBA Guidelines. For example:

- Section 6.4 sets out the list of topics/headings which should be considered but without absolute prescription as to what the clauses should ultimately state. For example, it is said that firms "may" elect to limit contractual termination rights to situations such as "material" breaches of law, regulation or contractual provisions or risks beyond the firm's tolerance. This appears to be materially more flexible than the equivalent EBA statement as to termination rights in section 13.4 of the EBA Guidelines.
- Whilst the detail of the audit requirements appears to mirror that in the EBA Guidelines, an important difference is that SS2/21 states that the obligation upon the firm is to take "reasonable steps" to procure the inclusion of the relevant audit provisions in the final written agreement, rather than the outright obligation to "ensure" their inclusion, as appears in section 13.3 of the EBA Guidelines. It appears that the PRA will also be more amenable to the use of pooled audits than the EBA might be, in that there is no absolute requirement that firms retain the right to undertake

individual audits, come what may (as whilst the right must be maintained to undertake additional information/audit access "where justified from legal, regulatory or risk management perspectives", SS2/21 states that such additional audits can be individual OR pooled).

- The restrictions regarding sub-outsourcing are applied to "material" sub-outsourcing (as per section 9) which helps resolve the doubt as to whether the EBA's equivalent provisions were intended to apply to ALL sub-outsourcings, or only those of critical or important functions.

There are at least no additional requirements beyond what the EBA Guidelines had envisaged, which will be a relief to those firms who are already some way in to their remediation programmes (albeit that – as noted above - they may now need to expand the scope of those programmes to cover services arrangements which are "material" but would not otherwise have been seen as a form of outsourcing). It is also worth noting that whilst SS2/21 will be the primary reference source for PRA requirements vis a vis outsourcing, the other existing regulations (et SYSC, MIFID II etc) also remain relevant and would need to be considered, albeit that they tend to be less prescriptive than the EBA Guidelines and now SS2/21 in any event.

The key differences between the EBA Guidelines on Outsourcing Agreement and SS2/21 are set out below.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Key concepts		
When does it come into force?	30 September 2019	31 March 2022. Outsourcing arrangements entered into ***on or after Wednesday 31 March 2021*** should meet the expectations in the SS by 31 March 2022. Outsourcing arrangements entered into ***before 31 March 2021*** should be reviewed and updated at the "first appropriate contractual renewal or revision point" so as to meet the requirements of the SS as soon as possible on or after 31 March 2022.
What does it implement?		The EBA Guidelines on outsourcing arrangements and some elements of the EBA Guidelines on ICT and security risk management.
What is the status of other applicable European guidelines / requirements?		The PRA is not implementing the following: • EIOPA Guidelines on outsourcing to cloud service providers • EIOPA Guidelines on information and communication technology security and governance • ESMA Guidelines on outsourcing to cloud service providers.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
		The SS should be the primary reference point for UK firms when ascertaining the requirements of the PRA. Firms with operations in both the UK and the EU should comply with the applicable Guidelines in respect of their EU operations. The SS also sets out a range of other requirements (at both an European and UK level) that firms need to take into account and adhere to.
To whom does it apply?	Broadly: credit institutions meaning banks; MiFID investment firms; payment institutions and electronic money institutions.	UK banks, building societies and PRA-designated investment firms, plus insurance, reinsurance firms and groups within the scope of Solvency II, including the Society of Lloyd's and managing agents; and UK branches of overseas banks and insurers.
Does it cover intra-group arrangements?	The guidelines apply to intra-group arrangements.	Principles apply on same basis as if service provider was outside the group **but** requirements can be applied proportionately depending on level of "*control and influence*" exercised by customer. Outsourcing to an overseas intra-group company needs to comply with UK legal and regulatory requirements.
To what does it apply?	Arrangements within the EBA's definition of "*outsourcing*": see definition below.	Arrangements within the PRA's definition of "*outsourcing*": see definition below, together with some other third party arrangements
How is "*Outsourcing*" defined?	A provider which "*performs a process, a service or an activity that would otherwise be undertaken by the [customer] itself*". There should be some characteristic of recurrence or ongoing supply to help to distinguish the service from purchasing. There is a list of arrangements that "*as a general principle*" would not be considered outsourcing.	The PRA Handbook defines outsourcing as: "*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*" . Consideration should be given to whether the third party will perform the relevant function or service on a recurrent or ongoing basis. The SS also provides that there are a number of arrangements which "as a general principle" should not be considered as outsourcing (known as "non-outsourcing third party arrangements"). These are: • Purchase of hardware, software and other ICT products, including: – Design and build of an on-premise IT platform

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
		– Purchase of data from third party providers – "off the shelf" machine learning models including samples of the data used to train and test the models, OSS and machine learning libraries developed by third party providers. In the case of insurers, the use of aggregators, and delegated underwriting.
How is cloud treated?		It is *not automatically deemed* as a form of outsourcing. There is some specific guidance to help firms to deploy cloud "*in a safe and resilient manner*". In particular, the SS recognises the shared responsibility model in respect of data outsourced to the cloud; whereby: • the firm is responsible for what is in the cloud and the service provider is responsible for the cloud; • firms are responsible for identifying and classifying data in line with regulatory obligations, and for configuration and monitoring of the data to reduce security and compliance incidents; and • cloud service providers assume responsibility for the infrastructure running the outsourced service e.g. data centres, hardware, software etc.
What is the materiality threshold?	Uses the term "*critical or important*". Certain requirements apply only to outsourcings that are critical or important.	Uses the term "*material*", leveraging the existing definition in the PRA Handbook, being "*services of such importance that weakness, or failure, of the services would cast serious doubt upon the firm's continuing satisfaction of the threshold conditions or compliance with the Fundamental Rules*" Outsourcing of services to which OCIR applies will generally constitute "material outsourcing", as will (amongst other criteria) outsourcing of services that involves an entire "regulated activity" e.g. portfolio management or "internal control " or "key function", unless the firm is satisfied a defect or failure would not adversely affect the relevant function.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Other relevant materiality criteria		The SS sets out a description of the materiality criteria to be assessed, including: • direct connection to the performance of a regulated activity; • size and complexity of relevant business area / function; • potential impact on business continuity, operational resilience, operational risk or ability to comply with legal / regulatory requirements (including those under the PRA handbook and under GDPR); • impact on policyholders, customers and counterparties; • potential impact on resolvability, RRP and resolvability; • the firm's ability to scale up the outsourced services; and • ability to substitute a service provider or bring the function back in-house, in terms of operational impact, costs, risk and timeframes.
Application of the proportionality principle	In applying the requirements, the institution should take into account the complexity of the outsourced functions, the risks arising from the outsourcing arrangement, the criticality or importance of the outsourced function and the political impact of the outsourcing on the continuity of their activities.	Firms are expected to meet the expectations in the CP/SS in a manner appropriate to their size and internal organisation and the nature, scope and complexity of their activities in line with the principle of proportionality. Proportionality looks to the characteristics of the firm and its systemic importance; materiality is different: looking instead at the impact of the outsourcing of the regulated entity's operations.
Notification		The PRA should be notified when "*entering, or significantly changing a material outsourcing arrangement*". The notification should be made in advance, and in respect of changed circumstances that bring the outsourcing arrangement within these parameters.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
		The timeliness of the notification will be a factor in considering whether a firm has complied with Fundamental Rule 7 (i.e. that the firm should deal with its regulators in an open and co-operative way, and must disclose to the PRA appropriately anything relating to the firm of which the PRA would reasonably expect notice).
Concentration Risk		Firms should assess and take reasonable steps to manage concentration risk and vendor lock-in due to: • multiple arrangements with the same or closely connected service providers; • fourth party / supply chain dependencies, where otherwise unconnected service providers rely on the same subcontractor; • arrangements which are difficult or impossible to substitute; and • concentration of outsourcing in a close geographical location, such as one jurisdiction, even in respect of multiple, unconnected third party service providers.
The outsourcing agreement for critical or important (EBA) / material (PRA) functions should set out (the differences being emphasised (by us) in bold, and the strikethrough / underlined text show the principal differences between the CP30/19 and the SS2/21):		
Services	A clear description of the outsourced function to be provided [75a].	A clear description of the outsourced function **including the type of support services** [6.4].
Dates	The start date, end date and, where applicable, notice periods for both parties [75b].	The start date, **next renewal date**, end date and termination notice periods for both parties [6.4].
Law	Governing law [75c].	~~**Court jurisdiction** and~~ governing law [6.5].
Charges	Financial obligations [75d].	Financial obligations [6.4].

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Sub-outsourcing	Whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, **the conditions specified in s.13.1 that the sub-outsourcing is subject to** [75e].	Whether the sub-outsourcing of a material function or part thereof, is permitted and, if so, **under which conditions** [6.4].
Location	The location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including a requirement to notify the customer if the provider proposes to change the location [75f].	The location(s) (i.e. regions or countries) where the material function **or service** will be provided and/or where relevant data will be kept ~~and **stored**~~**,** processed **or transferred**, including the possible storage location and a requirement **for the provider** to notify the customer **in advance** if the provider proposes to change ~~the~~ said location [6.4].
Data	**Where relevant,** provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, in accordance with the requirement of section 13.2 of the Guidelines [75g].	Provisions regarding the accessibility, availability, integrity, **confidentiality,** privacy and safety of relevant data [6.4].
Performance monitoring	Customer's right to monitor performance on an ongoing basis [75h].	Customer's right to monitor performance on an ongoing basis **(by reference to key performance indicators (KPIs))** [6.4].
Service Levels	Agreed service levels, which should include **precise,** quantitative and qualitative performance **targets** … to allow timely monitoring so that appropriate corrective action can be taken **without undue delay** if the agreed service levels are not met [75i].	Agreed service levels, which should include qualitative and quantitative performance **criteria** and allow for timely monitoring, so that appropriate corrective action can be taken if these service levels are not met [6.4].

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Reporting Obligations	Reporting obligations … including provider **communication** of any development that may have a material impact on its ability to effectively **carry out** the critical or important function in line with the service levels, compliance with law and regulatory requirements **and, as appropriate, obligations to submit reports of the provider's internal audit function** [75j].	Reporting obligations … including a requirement to **notify** the firm of any development that may have a material impact on the provider's ability to effectively **perform** the material function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements [6.4].
Insurance	Whether the provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested [75j].	Whether the provider should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested [6.4].
Business Continuity	Requirements to implement, and also to test, business continuity plans [75l].	Requirements **for both parties** to implement and test business continuity plans, **which should take account of firms' impact tolerances for important business services. This should include a commitment on both parties to take reasonable steps to support the testing of such plans** [6.4].
Continued access to data	Provisions to ensure that the customer's data can be accessed in case of provider insolvency, resolution or discontinuation of business operations [75m].	Provisions to ensure that the customer's data can be accessed **promptly** in case of provider insolvency, resolution or discontinuation of business operations of the service provider [6.4].
Co-operation	Obligation of provider to cooperate with regulators and resolution authorities, including others appointed by them [75n].	Obligation of the service provider to cooperate with the PRA and the Bank of England, as resolution authority, including others appointed by them [6.4].

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
BRRD	Clear reference to the national authority's powers, especially art. 68 + 71 BRRD and, in particular, a description of the "*substantive obligations*" of the contract in the sense of art.68 of the BRRD Directive [75o].	For banks, a clear reference to the Bank of England's resolution powers especially under s.48Z and 70C-D of the Banking Act 2009 (implementing a. 68 + 71 of the BRRD, and in particular a description of the "*substantive obligations*" of the written agreement in the sense of art. 68) [6.4].
Data security	Not included in the list of contractual requirements but the Guidelines do require that the service providers comply with appropriate IT security standards and "where relevant", the customer should define data and system security requirements within the Agreement and monitor compliance on an ongoing basis (s. 13.2)	**If relevant:** • **appropriate and proportionate information security related objectives and measures including requirements such as minimum cybersecurity ICT requirements, specifications of customer's data life cycle, and any requirements regarding to data security, network security and security monitoring processes; and** • **operational and security incident handling procedures including escalation and reporting.**
Termination	The termination rights specified in s. 13.4 [75q]; see below. Additionally, the institutions should have a documented exit strategy regarding critical or important functions, and develop comprehensive documentation and share appropriate, sufficiently tested exit plans.	Termination rights **and exit strategies covering both stressed and non-stressed scenarios** (which themselves are described in more detail in the consultation paper). **Both parties should commit to take reasonable steps to support the testing of customer's termination plans.** Firms may elect to limit contractual termination rights to situations such as: • material breaches of law, regulation or contractual provisions; • those that create risks beyond their tolerance; or • those that are not adequately notified and remediated in a timely manner.
Notification of non-compliance with the contractual requirements		If a service provider in a material outsourcing arrangement is unable or unwilling to contractually facilitate a firm's compliance with its regulatory obligations and expectations, including those set out above (as set out in para 6.4 of the SS2/21), the firm should make the PRA aware of this.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Termination and exit [1]		
Termination rights	The outgoing agreement should provide for the ability of the customer to terminate the outsourcing agreement in the case of:	
	Provider breach of law, regulation or contract [98a]	*Please see above.*
	Where impediments capable of altering the performance of the outsourced function are identified [78b]	
	Where there are material changes affecting the outsourcing arrangement or the provider (eg sub-outsourcing or change of sub-contractor) [98c]	
	Where there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information [98d]; and	
	On the instruction by the regulator [98e].	
Audit and Inspection		
Audit	The customer should ensure the agreement provides that the initial audit function is able to review the outsourced function using a risk based approach.	Firms should adopt a risk based approach to access, audit and information rights in respect of non-material outsourcing arrangements.

[1] These EBA requirements read in standalone seem to apply to all outsourcings but, in fact, are requirements flowing from 75 q (critical or important outsourcing agreements).

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
	Where the outsourcing is of a critical or important function the agreement should ensure the customer, regulators, resolution authorities, and others appointed by the customer or regulator [87] are granted:	For material outsourcing arrangements, the firm must take "*reasonable steps to ensure*" that the agreement provides customers, their **auditors**, the PRA and the Bank of England (as a resolution authority) and any other person appointed by the customer, PRA or Bank of England with "full access and unrestricted rights for audit and information to enable firms to: • comply with their legal and regulatory obligations and • monitor the arrangement [8.3].
	"***full access to all relevant business premises (e.g. head offices and operation centres),*** *including the* ***full range of*** *relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors*" [87a]; and	The right to audit in material outsourcing arrangements should include where relevant: • data, devices, information, systems and networks used for providing the outsourced service **or monitoring its performance**. This may include, where appropriate, the service provider's policies, processes and controls on data ethics, data governance and data security. • ~~the firms' ability to carry out~~ **the results of security penetration testing** carried out by the outsourced service provider or on its behalf, on its applications, data and systems to "*assess the effectiveness of implemented cyber and internal IT security measures and processes*" • **company and** financial information; and • the provider's external auditors, **personnel and premises.** [8.4]
	"*unrestricted rights of inspection and auditing related to the outsourcing arrangement to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements*".	

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Sub-outsourcing		
For sub-outsourcing of critical or important / material functions the agreement should set out:		
Definition of "sub-outsourcing"	*"A situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider"*	Under the PRA Rulebook, a situation where "*a service provider may perform a process, service or any activity which would otherwise be undertaken by the firm itself […] directly or by sub-outsourcing*" [9.1]
Permission	Whether or not the sub-outsourcing of critical or important functions (or material parts) is permitted [76].	whether or not material sub-outsourcing is permitted [9.9].
	Which activities are excluded from sub-outsourcing [78a].	any activities that cannot be sub-outsourced [9.9].
Conditions	the conditions to be complied with in the case of sub-outsourcing [78b].	the conditions to be complied with in the case of permissible sub-outsourcing, including to [9.9]:
Oversight	that the provider is obliged to oversee those services that is has sub-contracted[2] to ensure that that the contractual obligations between the provider and customer are continuously met [78c].	that the provider is obliged to oversee those services that it has sub-contracted[3] to ensure that all contractual obligations between the provider and customer are continuously met [9.8].
Consent	that the provider must obtain prior specific or general written authorisation before sub-outsourcing data [78d].	that the provider must to obtain prior specific or general written authorisation from the customer before transferring data (see art. 28 GDPR) and [9.9].

[2] Note the change in terminology to sub-contracting (not sub-outsourcing).

[3] As the footnote above.

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Prior notification	that the provider must **notify** the customer of planned or material changes to sub-outsourcing (incl. changes of sub-contractor or the notification period); and the notice period to allow the customer to be able to carry out a risk assessment and object before changes come in effect [78e].	that the provider must **inform** the customer of any planned or material changes to sub-outsourcing (incl. changes of sub-contractor or the notification period); and the notice period to allow the customer to be able to carry out a risk assessment and object before changes come in effect [9.9].
Right to object	ensure, where appropriate, that the customer has the right to object to intended sub-outsourcing, or material changes, or that explicit approval is required [78f].	ensure that, where appropriate, customers have the right to: • explicitly approve or object to the intended sub-outsourcing or material changes thereto: and [9.9].
Termination	ensure the customer has the contractual right to terminate for "*undue*" sub-outsourcing [(NB. this means without advance notice or where the sub-outsourcing materially increases risk)] [78g].	• ensure the customer has the contractual right to terminate the agreement in the case of specific circumstances, e.g. where the sub-outsourcing materially increases the risks for the customer or where the provider sub-outsources without notifying the customer [9.9]. A fuller list of potential termination rights is also provided in SS2/21.
Firms should only agree to sub-outsourcing if:		
No undue operational risk		the sub-outsourcing will not give rise to undue operational risk for the firm in line with Outsourcing 2.1(1) (banks) and Conditions Governing Business 7.2(2) (insurers);
Compliance with Law and contract	the sub-contractor undertakes to comply with all applicable laws, regulatory requirements and contractual obligations. [79a]	sub-outsourcing service providers undertake to comply with all applicable laws, regulatory requirements and contractual obligations. [9.5]

ISSUE	EBA GUIDELINES ON OUTSOURCING AGREEMENTS	SUPERVISORY STATEMENT (SS2/21) ON OUTSOURCING AND THIRD PARTY RISK MANAGEMENT
Audit	the sub-contractor must grant the customer and competent authority the same contractual rights of access and audit as those granted by the provider [79b].	sub-outsourcing service providers undertake to grant the customer, Bank of England and PRA equivalent contractual access, audit and **information rights** to those granted to [*sic*] the provider [9.5].

For further information please contact the authors:

Duncan Pithouse

Partner

duncan.pithouse@dlapiper.com

T: +44 (0) 20 7153 7264

M: +44 (0) 7738 295 307

Kit Burden

Partner

kit.burden@dlapiper.com

T:+44 (0) 20 7796 6075

M: + 44 (0) 7968 558 727

DGP/UKDP/UKM/109093398.1

www.dlapiper.com