Bank of England

Appendix 6: Outsourcing and third-party risk management Supervisory Statement: recognised payment system operators and specified service providers

December 2024

Outsourcing and third-party risk management Supervisory Statement: recognised payment system operators and specified service providers

1: Introduction

1.1 This Supervisory Statement (SS) on outsourcing and third-party risk management is relevant to the operators of payments systems recognised (RPSOs) under section 184 of the Banking Act 2009 (the Act) and specified service providers (SSPs) under section 206A of the Act. The 'Outsourcing and third party risk management: recognised payment system operators and specified service providers' part of the Code of Practice (the code) published under section 189 of the Act only applies to relevant RPSOs and SSPs.

1.2 The code does not apply to a recognised payment system that is operated by a central counterparty (CCP) or central securities depository (CSD). This is because the CCP or CSD will be subject to the expectations in the Bank's SS 'Outsourcing and third party risk management: central counterparties', and the Bank's SS 'Outsourcing and third party risk management: central securities depositories'. The Bank accepts that a CCP or CSD meeting those expectations will produce an appropriate and equivalent outcome in respect of the operational resilience of its embedded payment systems.

1.3 In respect of a RPSO or SSP that is incorporated outside of the UK, the Bank will determine on a case-by-case basis whether this RPSO or SSP will be subject to the Outsourcing and Risk Management Part of the Code of Practice and expectations, taking into account factors such as systemic importance in the UK and the extent to which the local (home-country) regulatory and supervisory framework delivers an equivalent outcome in terms of outsourcing and third party risk management.

1.4 This SS explains the Bank's supervisory approach to outsourcing and third-party risk management, which is relevant to many areas of a RPSO's and SSP's operations. It also provides guidance as to how the Bank expects RPSOs and SSPs to meet their regulatory obligations under the code and sets out more specific requirements and expectations for

RPSOs and SSPs than is contained within the Principles for Financial Market Infrastructures (PFMI). In particular:

- Chapter 2 elaborates on the definition of 'third party' and 'outsourcing' in the outsourcing and third party-risk management part of the code, and sets out the expectations for managing the risks arising from all third-party dependencies that could ~~can~~ pose a threat to the safety and efficiency of the payment system, thereby impacting financial stability. It also elaborates on the requirement for RPSOs to have a sufficient understanding of the risks to the end-to-end flow of the payments across the payment system when participants outsource their payment connectivity to the cloud.
- Chapter 3 clarifies how the principle of proportionality applies to the expectations in this SS, in particular, to intragroup outsourcing.
- Chapter 4 sets out the Bank's expectations on governance and accountability, risk management and record keeping.
- Chapter 5 sets out the Bank's expectations for RPSOs and SSPs during the pre-outsourcing phase. It addresses the materiality ~~criticality~~ and risk assessments of their outsourcing and other third-party arrangements (including notification to the Bank where required), and RPSOs' and SSPs' due diligence on third parties.
- Chapter 6 lists the areas that the Bank expects written agreements relating to material ~~critical~~ outsourcing arrangements to address as a minimum. The following four areas are then examined in detail in Chapters 7–10:
    - data security (Chapter 7);
    - access, audit, and information rights (Chapter 8);
    - sub-outsourcing (Chapter 9); and
    - business continuity and exit strategies (Chapter 10).

1.5 Pursuant to section 188 of the Act, the Bank adopted the PFMIs as a published set of principles in 2012 to which RPSOs are required to have regard, and these will continue to apply. In addition, the Bank requires SSPs specified under the Act to have regard to Annex F (Oversight expectations applicable to critical service providers) of the PFMI, which will also continue to apply.

1.6 The code will provide transparency on the minimum requirements that must be met by all RPSOs and SSPs to which the code applies. The new part of the code will be issued under section 189 of the Act; this means that it is binding on RPSOs and SSPs to which it applies. If a RPSO or SSP fails to comply with its requirements, the Bank may take enforcement action against it. The Bank's enforcement powers are set out in sections 196–202A of the Act.

1.7 These requirements and expectations also complement the '**Bank of England policy on Operational Resilience of FMIs**' published in March 2021 and the Bank of England policy on Operational Resilience: Incident and Outsourcing and Third Party Reporting for FMIs.

1.8 In addition, RPSOs and SSPs are expected to comply with the expectations in this SS by 9 February 2024. ~~Outsourcing arrangements entered into on or after 8 February 2023 should meet the expectations in this SS by 9 February 2024. RPSOs and SSPs should seek to review and update legacy outsourcing agreements entered into before 8 February 2023 at the first appropriate contractual renewal or revision point to meet the expectations in this SS as soon as possible on or after 9 February 2024.~~

1.9 In developing the expectations in this SS, including in relation to cloud usage, the Bank has taken account of:

- Financial Stability Board (FSB), 'Effective Practices for Cyber Incident Response and Recovery' (FSB Effective Practices) and Discussion Paper on 'Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships'.
- G-7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector' (G-7 Third Party Elements).
- International Organisation of Securities Commissions' (IOSCO) 'Principles on Outsourcing'.

1.10 The SS applies to all forms of outsourcing and, where indicated, third- party arrangements. This SS also includes examples, references and sections addressing specific issues of particular relevance to cloud outsourcing, such as data security, business continuity and exit planning. By addressing these issues, the SS seeks to provide conditions that can help give RPSOs or SSPs assurance to deploy the cloud in a safe and resilient manner in line with the Bank's response to **'The future of finance report'**.

1.11 This SS should be read in conjunction with the code. To promote clarity and certainty, this SS references other guidelines that govern outsourcing and third- party arrangements by RPSOs and SSPs. RPSOs and SSPs are expected to comply with the obligations in these sources. This SS should therefore be read alongside and interpreted consistently with the relevant oversight framework, including those in Table A.

Table A: Existing expectations and requirements on outsourcing and third-party risk management for RPSOs and SSPs

RPSOs	SSPs
Operational resilience part of the Code of Practice and operational resilience supervisory statement.	Operational resilience part of the Code of Practice and operational resilience supervisory statement.
CPMI-IOSCO Oversight expectations applicable to critical service providers (Annex F).	CPMI-IOSCO Oversight expectations applicable to critical service providers (Annex F).
CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI).	
Rules 2 and 3 in Part 4of Code of Practice for RPSO and SSPs on Notifications and Regulatory Reporting	Rules 2 and 3 in 4 in Part 4 of Code of Practice for RPSO and SSPs on Notifications and Regulatory Reporting

2: Definitions and scope

Third party~~ies~~ arrangments

2.1 The Bank defines third party~~ies~~ arrangements as any arrangments where a person ~~organisations, whether supervised entities or not, that have entered into business relationships or contracts with an RPSO or SSP to~~ provide products, services, processes, activities or business functions to an RPSO or SSP.~~, whether in whole or in part, including providers of utilities and other services~~ This is regardless of whether these products or services are ones that would otherwise be provided by the RPSO or SSP itself, are provided directly or by a sub-contractor, or are provided by a group entity, meaning that it encompasses both outsourcing and non-outsourcing third-party arrangements. This definition of 'third party' is consistent with the definition used by the G-7 Third-Party Elements and other international supervisory authorities. The scope of the SS includes products, services, processes, activities or business functions performed or provided by third parties, including both outsourced and non-outsourced arrangements. A RPSO or SSP will remain responsible if a third party on whom it relies, whether wholly or in part, to provide an important business service, fails to remain within impact tolerances or causes the RPSO or SSP to fail to do so.

Outsourcing arrangements

2.2 One type of third party arrangement is outsourcing. In line with the definition of third-party, the SS defines outsourcing as an arrangement of any form between an RPSO or SSP, and a third party, whether a supervised entity or not, by which that third-party provides a product, performs a service, a process, an activity or a business function, whether directly or by sub-outsourcing, which would otherwise be undertaken by the RPSO or SSP itself.

2.3 This definition expands on PFMI Principle 17: Operational Risk. A RPSO that relies upon or outsources some or all of its operations to a third party should ensure that those operations meet the same requirements they would need to meet if they were provided internally.

2.4 RPSOs and SSPs that enter into outsourcing arrangements remain fully accountable for complying with all their regulatory obligations. This is a key principle underlying all requirements and expectations regarding outsourcing and other third-party arrangements.

Non-outsourcing third-party arrangements

2.5 As some non-outsourcing third-party arrangements may also impact the Bank's objectives, the Bank expects RPSOs and SSPs to assess the risks of all third-party arrangements irrespective of whether they fall within the definition of outsourcing. RPSOs and SSPs, as risk managers, should apply adequate governance, risk management and controls to manage the risks arising from all their third-party arrangements that could pose a threat to the safety and efficiency of the payment system thereby impacting financial stability.

2.6 Examples of non-outsourcing third-party arrangements may include but are not limited to:

- purchases of hardware, software, and other information, communication and technology products such as:
  - the design and build of an on-premise IT platform;
  - the purchase of data collated by third party providers (data brokers);
  - open source software, and machine learning libraries developed by third-party providers;
  - the use of aggregators or facilitators to access another financial market infrastructure; and
  - the use of a supply chain for the provision of hardware, and other information, communication and technology products.

2.7 Third-party arrangements are also subject to relevant requirements on operational resilience. Where third parties provide or support the provision of important business services, the Bank expects RPSOs and SSPs to manage the risk and obtain appropriate assurance to ensure important business services are able to remain within impact tolerance in the event of an extreme but plausible disruption.

Material ~~Critical~~ third-party~~ies~~ and material ~~critical~~ outsourcing arrangements

2.8 The Bank defines material ~~critical~~ third party~~ies~~ arrangments, for the purposes of this SS, as those where the disruption or failure of the products of services that they provide to the RPSO or SSP could pose a risk to the continuity of service provided by the RPSO or SSP, or the safety and efficiency of the RPSO or SSP's delivery of their services ~~continuous, secure and efficient delivery of their services to RPSOs or SSPs is critical to the operation of the RPSO or SSP[1]~~. This is irrespective of whether the relationship is an outsourced or non-outsourced arrangement. This definition builds on Annex F where the operational reliability of a RPSO or SSP may be dependent on the continuous and adequate functioning of such third-party arrangements. This definition of materiality ~~criticality~~ extends to outsourcing arrangements and other third-party arrangements, where the relevant services are of such

[1] ~~The Bank, Prudential Regulation Authority (PRA) and Financial Conduct Authority's (FCA's) forthcoming joint Discussion Paper on Critical Third Parties would consider those third parties that may be a source of systemic risk to the financial stability of the UK. While we also refer to critical third parties in this SS, this definition should be understood to refer to how financial market infrastructures (FMIs) classify their own third party and outsourcing arrangements as opposed to third parties that could be designated as 'critical' under any future regulatory framework.~~

importance that a disruption ~~weakness~~, or failure, of the services could ~~would~~ pose a risk to the continuity of service provided by the RPSO or SSP, and could threaten the safety and efficiency of payment systems.

2.9 Where a third-party arrangement is identified as a material critical third-party arrangement, RPSOs and SSPs must comply with the Bank's Notification and Regulatory Reporting Code of Practice, and the Bank expects RPSOs and SSPs to meet the expectations set out in Annex F, and implement proportionate, risk-based suitable controls. These controls do not necessarily have to be the same as those that apply to outsourcing arrangements. However, the controls should be appropriate to the risks of the third-party arrangement and as robust as the controls that would apply to outsourcing arrangements with an equivalent level of risk. It follows that RPSOs or SSPs should apply stricter controls to high risk, non-outsourcing third-party arrangements than to low risk outsourcing arrangements.

Participant outsourcing arrangements

2.10 Where RPSOs permit participants to outsource their connectivity to financial markets infrastructure to the cloud, this may create indirect dependencies on one or more cloud service providers (CSPs), with which a RPSO may or may not have a separate, direct contractual relationship (and by extension, concentration risk on a single provider at both the RPSO and systemic levels). RPSOs act as risk managers and should therefore understand the nature and scope of outsourcing among their participants, including how the use of new technologies, such as the cloud, may introduce new, or increase existing, systemic risks. This is consistent with the requirement set out in the code, Paragraph 2.3, where the RPSO should ensure that it has a sufficient understanding of the risks to the end-to-end flow of payments across the payment system.

2.11 This is also consistent with PFMI Principle 3 – Framework for comprehensive management of risks and Principle 18 – Access and participation requirements, and the Bank therefore expects RPSOs to have regard to these principles by demonstrating effective governance, and that they are able to manage their ecosystem to set, monitor and enforce standards, including those relating to information security and operational resilience.

Important business services

2.12 The operational resilience part of the code requires RPSOs and SSPs to identify their important business services, and document the necessary people, processes, technology, facilities, and information (the resources) required to deliver each of their important business services. This process is referred to as mapping. The Bank expects RPSOs and SSPs to map the resources necessary to deliver important business services including where the resources are being provided wholly or in part by a third party, or in an intragroup entity.

RPSOs and SSPs should identify and understand how their third parties support their important business services, including any reliance placed on supply chains or sub-outsourcing arrangements. Important business service is defined in the operational resilience part of the code, where in respect of a:

- RPSO, is a service provided by the RPSO to an end-user which, if disrupted, could threaten the transfer of payment or safety and efficiency of a payment system; and
- SSP, is a service provided by a SSP to a RPSO which, if disrupted, could threaten the transfer of payment or safety and efficiency of the RPSO.

2.13 The operational resilience part of the Code of Practice also requires RPSOs and SSPs to set an impact tolerance for each of its important business services. The impact tolerance must be set for each important business service at a maximum tolerable level of disruption, whereby further disruption would threaten the safety and efficiency of the payment system. RPSOs and SSPs must take all reasonable actions to ensure it remains within its impact tolerance for each important business service in the event of an extreme but plausible disruption to its operations.

3: Proportionality

3.1 RPSOs and SSPs should meet the expectations in this SS in a manner appropriate to their size, internal organisation, risk profile, and the nature, scope and complexity of their activities.

3.2 Proportionality and the materiality ~~criticality~~ of outsourcing arrangements (see Chapter 5) are separate but complementary concepts, and RPSOs and SSPs should consider the links between the two. Proportionality focuses on the characteristics of a RPSO or SSP, including its systemic significance. Materiality ~~Criticality~~ assesses the potential impact of a given outsourcing or third-party arrangement on the safety and efficiency of the payment system, including: its operational resilience; its ability to comply with legal and regulatory obligations; and the risk that RPSOs' or SSPs' ability to meet these obligations could be compromised if the arrangement is not subject to appropriate controls and oversight. Materiality ~~Criticality~~ can change over time, RPSOs and SSPs should reassess both materiality ~~criticality~~ and proportionality as appropriate.

Intragroup outsourcing

3.3 Intragroup outsourcing is not inherently less risky than outsourcing to third-parties outside a RPSO's or SSP's group, and is subject to the same expectations. RPSOs and SSPs should have due regard to the level of control and influence it has over the entity that is providing the outsourced service, and comply with the requirements in the SS in a proportionate manner.

3.4 Control and influence may vary depending on the characteristics of a group. For instance, a RPSO that outsources to a subsidiary may have greater control and influence than one that outsources to its parent company. The following factors may also be relevant when determining the level of control and influence:

- the group's governance structure, including reporting lines, the level of connectivity between a RPSO's or SSP's and its group's boards, board committees, executive committees, internal control functions and/or other relevant functions (eg technology or shared services);
- the allocation of responsibilities throughout the group;
- the ability of a RPSO or SSP to alter its intragroup outsourcing arrangements and/or influence their terms and conditions to ensure they meet its UK regulatory obligations and manage the relevant RPSO's or SSP's business and UK-specific risks; and
- the consistency and robustness of group wide standards, controls, policies, and procedures (eg on business continuity plans and cyber security).

3.5 Depending on its level of control and influence in respect of intragroup outsourcing arrangements, a RPSO or SSP may, for example:

- rely on the vendor due diligence undertaken by the group, although the RPSO or SSP should still be fully accountable for assessing and deciding whether a potential third party that is part of its group has the ability, capacity, resources, and appropriate organisational structure to support the performance of the outsourced function or third-party service;
- rely on the group's potentially stronger negotiating and purchasing power to enter into group-wide arrangements with external third parties;
- adapt certain clauses in outsourcing agreements (a written agreement is always required – even in intragroup arrangements; see Chapter 6);
- rely on group policies and procedures, as long as they comply with its UK legal and regulatory obligations and allows it to manage relevant risks (eg group cyber security or data protection policies, such as binding corporate rules for international data transfers);
- rely on a centralised group process for overseeing third parties, including the exercise of access, audit, and information rights, provided that this process appropriately takes into account and documents any legal entity-specific risks and allows for legal entity-specific risk mitigation where necessary; and
- rely on business continuity, contingency, and exit plans developed at group level, provided that they adequately safeguard the RPSO or SSP's operational resilience (eg where the outsourcing or third-party arrangement supports the delivery of an important business service, the group's business continuity policy sets out a recovery objective that is consistent with the impact tolerance assigned to that important business service).

4: Governance and record keeping

4.1 The Bank sets out expectations in this SS regarding:

- board engagement on outsourcing and third-party risks;
- outsourcing and third-party risk management;
- allocation of responsibilities;
- outsourcing and third-party risk management policies; and
- record-keeping.

4.2 The term 'board' is consistent with the definition set out in the governance part of the code. It is defined as a RPSO's or SSP's body or bodies appointed in accordance with national law, which are empowered to set a RPSO's or SSP's strategy, objectives and overall direction, oversee and monitor executive decision-making, and includes the people who effectively direct the business of a RPSO or SSP. This section builds on the governance part of the code on expectations in relation to outsourcing and third party risks.

Board engagement on outsourcing and third party risks

4.3 Boards and senior management cannot outsource their responsibilities. RPSOs and SSPs that enter into outsourcing arrangements remain fully accountable for complying with all their regulatory obligations. This is a key principle underlying all requirements and expectations regarding outsourcing and non-outsourcing third-party arrangements, including the expectations in this SS.

4.4 Building on PFMI Principle 2: Governance, RPSOs boards should establish a clear, documented risk management framework that includes its risk tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision-making in crises and emergencies. Consistent with Annex F, SSPs are also expected to identify and manage relevant operational and financial risks to their critical services, and ensure that their risk management processes are effective. Governance arrangements should ensure that the risk management and internal control functions have sufficient authority, independence, resources, and access to the board. A RPSO's or SSP's board, or a body designated by the board with responsibility for risk management should:

- set the control environment throughout the RPSO or SSP, including the risk appetite or tolerance levels in respect of outsourcing and third-party risk management; and
- bear responsibility for the effective management of all risks to which the RPSO or SSP is exposed, including by:
    - approving the criteria used for assessing and identifying third parties and outsourcing arrangements that are critical to the RPSO and SSP;

- appropriately identifying and having an understanding of the RPSO's or SSP's reliance on material ~~critical~~ third parties and materiality ~~critical~~ outsourcing arrangements;
- ensuring that the RPSO or SSP has appropriate and effective risk management systems and strategies in place to deal with outsourcing arrangements and the third parties; and
- ensuring that appropriate risk mitigation steps have been taken where a third party provider on whom it relies, whether wholly or in part, to provide an important business service, is unable to remain within impact tolerance in the event of an extreme but plausible disruption event.

4.5 In line with the code, the Bank expects RPSOs to perform the function of a risk manager, and ensure that it has sufficient understanding of the risks to the end-to-end flow of payments across the payments systems. This includes being responsible for managing and mitigating risks that its third parties pose to the safety and efficiency of the payment system that may thereby impact the financial stability of the UK.

Outsourcing and third-party risk management framework

4.6 The code requires the RPSO's or SSP's board to approve and periodically review the risk management framework to ensure that it is fit for purpose. RPSOs and SSPs should thoroughly identify, assess, measure, monitor, and control the risks associated with their third parties to within board approved risk appetite. The Bank expects a RPSO and SSP to undertake an assessment of the operational risks arising from the delivery of any important business services that are provided or supported by third parties as well as operational risks arising from the use of information, communications or technology (ICT) systems. RPSOs and SSPs may leverage and build on oversight expectations set out in Annex F. Each RPSO or SSP is expected to demonstrate that operational risks and operational resilience issues are reflective of its risk profile, product offerings, business model and operational structure.

4.7 RPSOs and SSPs should ensure that key operational risks identified are considered in and/or managed by:

- the design of third-party detective, preventative and mitigation controls;
- an embedded risk and control self-assessment process set out in the operational risk management framework;
- specifying expectations, rights and obligations of third parties as part of contract structuring, business continuity and exit management strategy;
- monitoring the operational risks arising from any outsourcing arrangements performed by the third party; and

- the design of disruption scenarios involving third parties that are extreme but plausible, for the purposes of testing and managing the operational resilience of important business services.

4.8 RPSOs and SSPs should set triggers for reperforming risk assessments of third party and outsourcing arrangements to reaffirm that the third party and outsourcing risks remain within risk appetite, based on an up-to-date understanding of the risks. This should include: an assessment of potential cyber risks and vulnerabilities related to third parties; monitoring of risk metrics and risk indicators; assessment of emerging risks etc. If an RPSO or SSP leverages a third-party risk management framework used for assessing and managing third party and outsourcing risks, any risk policies, guidelines, standards and procedures should be aligned to the RPSO's or SSP's broader enterprise risk and operational risk management framework.

4.9 RPSOs and SSPs may also leverage their end-to-end mapping of important business services required under the operational resilience part of the code to identify their intragroup and other third-party dependencies.

4.10 As set out in the **Bank's supervisory statement on operational resilience for recognised payment system operators and specified service providers**, where a third party is unable to meet the impact tolerance set for any important business service, or where there is uncertainty as to whether it can be met, the Bank expects a RPSO or SSP to set out remedial actions that it will undertake to ensure the impact tolerance can be met at an agreed future date. In such situations, the Bank expects the RPSO or SSP to explain how such risks will be managed as part of its risk management framework; specifically, how mitigating actions, enhancements to the business continuity and disaster recovery plans, combined with testing, will ensure that the important business service can be brought within the impact tolerance should disruption reoccur. In addition, the Bank expects evidence that important business services assessed as being at risk of breaching its impact tolerance are prioritised when a RPSO or SSP makes investment decisions and choices about remediation or improvements in its systems, processes and technologies.

Shared responsibility model

4.11 As part of ensuring effective governance of an outsourcing arrangement, the Bank expects RPSOs and SSPs to define, document, and understand their and the third-parties' respective responsibilities. In the case of cloud computing, the term commonly used to help RPSOs or SSPs and cloud providers understand their respective obligations is the 'shared responsibility model'. An example of how the shared responsibility model operates in the case of data outsourced to CSPs is set out below.

Example of a shared responsibility model in cloud outsourcing

CSPs tend to operate under the ‘shared responsibility model’ whereby:

- RPSO or SSP is responsible for what is in the cloud and the CSP is responsible for the provision of the cloud;
- RPSO or SSP remains responsible for correctly identifying and classifying data in line with their legal and regulatory obligations, and adopting a risk based approach to the location of data. They also remain responsible for configuration and monitoring of their data in the cloud to reduce security and compliance incidents;
- CSP assumes responsibility for the infrastructure running the outsourced service, eg data centres, hardware, and software etc; and
- RPSO or SSP, and CSP share other responsibilities depending on the service model, eg Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), etc.

Accountability for outsourcing and third-party risks

4.12 In line with the requirements set out in the code, the board must ensure that members of the executive of a RPSO or SSP possess appropriate skills and experience necessary to discharge their responsibilities for the operation and risk management of the payment system, including managing the risks arising from outsourcing and third-party arrangements.

4.13 Where appropriate, RPSOs or SSPs should assign responsibility for third-party risk and outsourcing to an accountable person, either a board member and/or a senior executive. These responsibilities encompass the RPSO’s or SSP’s overall third-party risk management framework, policy, and systems and controls relating to outsourcing. The responsibility for individual outsourcing or third-party arrangements may still lie with relevant business lines or other functional areas of the RPSO or SSP.

4.14 Roles and responsibilities should be clearly defined for day-to-day oversight of third party and outsourcing arrangements. This includes periodic assessment against service level/contractual agreements, as well as of operational incidents and management performance metrics. There should also be an independent second-line review function to provide oversight and challenge. This should be complemented by a third-line internal audit function to provide assurance on internal control effectiveness of third-party risk management, and compliance with the relevant policies, legal and regulatory requirements.

Outsourcing and third-party risk management policies

4.15 In line with the requirements set out in the governance part of the code, RPSOs’ or SSPs’ boards should approve, regularly review, and implement a written third-party risk management policy, and where relevant, an outsourcing policy. This policy should align to and draw upon other relevant internal policies and strategies. A non-exhaustive list of policies that should be considered includes:

- business model and strategy;
- business continuity;
- conflicts of interest;
- data protection;
- information technology;
- cyber security;
- participant rule book or scheme rules;
- operational resilience; and
- risk management.

4.16 RPSOs and SSPs should make outsourced and third parties aware of relevant internal policies, including those on outsourcing, data protection, information technology, cyber security, and operational resilience. Where RPSOs' or SSPs' policies include confidential or sensitive information, RPSOs and SSPs should omit or redact it and only share those sections relevant to the performance of the outsourced or third-party service. If redacting or omitting sections of RPSOs' or SSPs' policies is not possible without compromising the readability of the original document, then RPSOs or SSPs should provide separate summaries of the omitted or redacted sections that are relevant to the performance of the outsourced or third-party service. Sharing these policies or summaries thereof with third parties does not dilute RPSOs' or SSPs' responsibilities in terms of managing their outsourcing and third-party arrangements but can help those third parties get a better understanding of RPSOs' and SSPs' regulatory obligations and other relevant aspects such as their risk tolerance and expected service levels.

4.17 RPSOs should also set out their policy and communicate their expectations (eg as part of the scheme rules or their rulebook) when participants engage in outsourcing arrangements that may create new risks to the payment system, or amplify existing risks. RPSOs should set out in their policy how the risks to the end-to-end flow of payments across the payment system may be mitigated. For example, when participants are permitted to outsource their connectivity to financial market infrastructure to the cloud, the safety, efficiency, and operational resilience of the payment system may be dependent on the relevant CSPs.

4.18 RPSOs' and SSPs' business continuity policies and plans should take in to account:

- the possibility that the quality of the provision of important business services that are outsourced services deteriorates to unacceptable levels;
- the possibility of a prolonged outage at the material ~~critical~~ third party;
- the potential impact of the insolvency or other failure of the material ~~critical~~ third party (see Chapter 10); and

- where relevant, political and other risks in the third-party's jurisdiction.

4.19 There is no 'one-size-fits-all' template for RPSOs' and SSPs' outsourcing and third-party risk management policies, and the policy does not have to be contained in a single document. RPSOs and SSPs are responsible for developing and maintaining a policy that is appropriate to their complexity, organisational structure, and size.

4.20 The outsourcing and third-party risk management policy should be principles-based and may be supported by detailed procedures developed, approved, and maintained below board level. However, it should be sufficiently detailed to provide adequate guidance for a RPSO's or SSP's staff on how to apply its requirements in practice. At a minimum, it should cover the areas in Table B.

Table B: Contents of outsourcing and third party-risk management policy

Section	Content covered
General	• The responsibilities of the board, including its involvement, as appropriate, in decisions regarding outsourcing to third parties. • The involvement of business lines, internal control functions, and other individuals in respect of outsourcing and third party arrangements. • Links to other relevant policies. • Documentation and record-keeping. • Procedures for the identification, assessment, management, and mitigation of potentially relevant conflicts of interest. • Business continuity planning (BCP) (see Chapter 10). • Differences, if any, between the approach to: ◦ intragroup outsourcing versus outsourcing to external third parties; ◦ material ~~critical~~ versus non- material ~~critical~~ outsourcing; ◦ outsourcing to third parties regulated or overseen by the Bank, PRA, or FCA versus unregulated third parties; and ◦ outsourcing to third parties in specific jurisdictions outside the UK.
Pre-outsourcing and on-boarding	• The processes for vendor due diligence and for assessing the materiality ~~criticality~~ and risks of outsourcing and third party arrangements (including notification to the Bank where required).

Section	Content covered
	• Responsibility for signing-off new outsourcing and third party arrangements, in particular material ~~critical~~ outsourcing arrangements.
Oversight	• Procedures for the ongoing assessment of third parties' performance, including where appropriate: ◦ day-to-day oversight, including incident reporting, periodic performance assessment against service level agreements, and periodic strategic assessments; ◦ being notified and responding to changes to an outsourcing or third party arrangement (eg to its financial position, organisational or ownership structures, or sub-outsourcing); ◦ an independent second-line review function and a third-line internal audit function to provide oversight/challenge, and assurance, of internal control effectiveness, compliance with policies, legal and regulatory requirements respectively; and ◦ renewal processes.
Termination	• Exit strategies and termination processes, including a requirement for a documented exit plan for critical outsourcing arrangements where such an exit is considered possible, explicitly catering for the unexpected termination of an outsourcing agreement (a stressed or unplanned exit), and taking into account possible service interruptions (and the RPSO's and SSP's impact tolerance for important business services) (see Chapter 10).
Participant outsourcing arrangement	• When participants engage in outsourcing arrangements that may create new risks to the payment system or amplify existing risks to the payment system, the RPSO or SSP should set out in their policy how the risks to the end-to-end flow of payments across the payment system may be identified, monitored and mitigated. These may include the use of requirements to set out rules on information security, operational resilience and business continuity. It may also require participants to test the resiliency of the arrangement, or the participants' response to a prolonged outage at their third party.

Section	Content covered
Incident response	• Procedures for incident response, including methods to detect and collect information about operational incidents originating at a third party, or at the RPSO or SSP affecting the third party. Procedure should also include communication strategy and reporting mechanisms with other stakeholders and authorities, and roles and responsibilities in any incident response plan.

Record keeping

4.21 The Bank expects RPSOs and SSPs to keep appropriate records of their outsourcing and third-party arrangements. The records must be sufficient to enable the RPSO and SSP to fulfil the expectations concerning concentration risk set out in Paragraph 5.19 below. In addition to the requirements set out in para 4.21A below, RPSOs and SSPs should also make any information on their outsourcing and third-party arrangements, of which the Bank would reasonably expect notice, available to it.

4.21A Rule 3 in Part 4 of the Code of Practice requires RPSOs/SSPs to maintain an up to date register of information on their material third party arrangements ('Register'). RPSOs/SSPs must submit the completed Register once and ensure this is kept up to date at least annually. The Bank expects RPSOs/SSPs to submit the Register and any updates through the FCA RegData portal. The Register collects the data groups specified in Table C.

4.21B For the purposes of completing the Register, the Bank does not expect RPSOs/SSPs to submit information on arrangements pertaining to basic utilities (e.g. electricity, gas, water

4.21C The Register template and associated guidance can be found in Appendix 9.

Table C: Data to be collected under the Register

Master data on regulated firms	Details on the firm submitting material third-party arrangement information, including firm identification and submission references.
Master data on third parties, including intra-group arrangements	Details of the third-party service provider firms have an arrangement with, including the name, registered address, and legal identifiers of the service provider.
Data on types of products or services being performed by a third party	Information on the products or services being provided by an external third-party provider, including a description of the product or service, whether the product or service supports an Important Business Service, and where the product or service is being performed.
Data on products and/or services used	Information on the type of product or service being provided by an external third party.

Information on supply chain	Ranking of third-party providers for each service included in the scope of each contractual arrangement. This includes information of the third-party provider name and LEI; and information of the receiving firm name and FRN.
Data on assessments	Information on the firm’s due diligence conducted for each arrangement, including details on risk assessments, recent audits, and reviewal from the appropriate Senior Management Functions.

The Bank may also request data on CCPs’ outsourcing arrangements using the information gathering powers under section 204 of the Banking Act 2009.

5: Pre-outsourcing phase: materiality ~~criticality~~ assessment, due diligence and risk assessment

5.1 The Bank requires RPSOs and SSPs to:

- Notify the Bank when entering, or significantly changing, a material third-party arrangement.

5.1A The Bank expects RPSOs and SSPs to:

- assess the materiality ~~criticality~~ of every outsourcing and third-party arrangement. Some criteria, or a combination of criteria, if met, would result in an expectation that the outsourcing or third-party arrangement should be automatically deemed material ~~critical~~;
- define an assessment framework, including the setting of thresholds or classification of materiality ~~criticality~~ that is aligned to the RPSO's or SSP's broader operational risk management framework, that is used for identifying and managing third-party risks;
- notify the Bank and seek the Bank's non-objection when entering, or significantly changing a material ~~critical~~ outsourcing or ~~third-party~~ arrangement, or when there is a material change in their risk profile, and that of the end-to-end flow of payments across the payment systems;
- Seek the Bank's non-objection when entering, or significantly changing a material third party arrangement, or when there is a material change in their risk profile, and that of the end-to-end flow of payments across the payment systems.
- perform appropriate and proportionate due diligence on all potential third-party arrangements, taking into account expectations set out in Annex F and where outsourcing involves an important business service, to take into account the requirements set out by the operational resilience part of the code to ensure the third party can maintain the relevant important business within the RPSO's or SSP's impact tolerances in the event of extreme but plausible disruption;
- assess the risks of every third-party arrangement, irrespective of materiality ~~criticality~~, by identifying the plausible sources of operational risks, including the potential risks arising from the dependency on all third party and outsourcing arrangements, and mitigate their impact through the use of appropriate systems, policies, procedures and controls; and
- set out an appropriate frequency to periodically (re)assess the materiality ~~criticality~~ of third-party arrangements. This should include taking reasonable and proportionate steps to identify and manage their overall reliance on third parties, monitor the risk of concentration and manage the risk of vendor lock-in.

Materiality ~~Criticality~~ assessment

5.2 The Bank's definition of 'material third party arrangements' is consistent with the PFMI definition~~es~~ third parties as being critical if the continuous, secure and efficient delivery of these services may be critical to the operations of the RPSO. The Bank's ~~is~~ definition of materiality ~~criticality~~ also extends to outsourcing arrangements and other third-party arrangements, where the relevant 'services are of such importance that a disruption ~~weakness~~, or failure, of the services could ~~would~~ pose a risk to the continuity of service provided by the RPSO or SSP, and could threaten the transfer of payments or the safety and efficiency of the payment system. The concept of material ~~critical~~ is consistent with the oversight expectations applicable to critical service providers in Annex F, and materiality, as defined in **PRA SS2/21 Outsourcing and third-party risk management** which applies to PRA-regulated firms.

5.3 The assessment of materiality ~~criticality~~ of outsourcing arrangements should also take into account whether the outsourcing impacts wholly, or in part, the provision of a RPSO's or SSP's important business services. If a RPSO or SSP outsources services that affects the delivery of important business services, this arrangement will generally constitute a 'material critical outsourcing arrangement'.

5.4 The concept of materiality criticality itself and the criteria in this chapter apply to all third-party arrangements. RPSOs and SSPs should determine the materiality criticality of all third-party arrangements using all relevant criteria in this chapter.

Timing and frequency of materiality ~~criticality~~ assessments

5.5 RPSOs and SSPs are expected to set out an appropriate frequency to periodically assess the materiality ~~criticality~~ of their outsourcing and third-party arrangements. Materiality ~~Criticality~~ may vary throughout the duration of an arrangement and should therefore be (re)assessed:

- prior to signing the written agreement;
- at appropriate pre-determined intervals thereafter eg during scheduled review periods;
- where a RPSO or SSP plans to scale up its use of the service or dependency on the third party;
- if a significant organisational change at the third party or a sub-outsourced third party takes place that could change the nature, scale, and complexity of the risks inherent in the outsourcing arrangement, including a significant change to the third party's ownership or financial position; and
- where a third party is identified as supporting an important business service following a review of the RPSO's or SSP's mapping or testing of important business services, or an operational incident.

5.6 Where a RPSO or SSP expects an outsourcing or third-party arrangement to become material ~~critical~~ in the future, it should take reasonable steps to ensure that it can comply with all applicable expectations in Chapters 6 to 10 before the materiality ~~criticality~~ threshold is crossed. If an outsourcing or third-party arrangement becomes material ~~critical~~ as a result of new information, changes to operational arrangements, or due to an unexpected occurrence of a severe event, such as a pandemic, RPSOs or SSPs should consider whether additional measures to safeguard their operational resilience are warranted, such as revisions to contractual provisions.

Criteria for assessing materiality ~~criticality~~

5.7 RPSOs and SSPs should develop their own processes for assessing materiality ~~criticality~~ as part of their outsourcing or third party-risk management policy. The assessment framework, including the setting of thresholds for classification of materiality ~~criticality~~, should be aligned to the RPSO's or SSP's broader operational risk management framework that is used for identifying and managing third-party risks. The Bank expects RPSOs and SSPs to generally consider an outsourcing or third-party arrangement as material ~~critical~~ where a disruption ~~defect~~ or failure in the ~~its~~ performance of the product or service provided to the RPSO or SSP could pose a risk:

- to the continuity of service provided by RPSO or SSP, or ~~threaten~~ the transfer of payments or safety and efficiency of a payment system, thereby threatening the financial stability of the UK; or
- impact the resolvability of the RPSO or SSP.

5.8 The Bank also expects RPSOs and SSPs to classify an outsourced or third-party arrangement as material ~~critical~~ if it involves an important business service or where there is a dependency on a third party for the delivery in part, or in full.

5.9 The Bank expects RPSOs and SSPs to have regard to all applicable criteria set out below, both individually and collectively, when assessing the materiality ~~criticality~~ of an outsourcing or third-party arrangement not otherwise covered in this chapter. Although in practice, many material ~~critical~~ outsourcing and third-party arrangements involve ICT products or services (eg cloud), the presence of a given ICT product or service does not, in itself, automatically render an outsourcing arrangement material ~~critical~~.

Materiality ~~Criticality~~ criteria

- Direct connection to the performance of a regulated activity.
- Size and complexity of relevant business area(s) or function(s).
- The **potential impact** of a disruption, failure, or inadequate performance on the RPSO's or SSP's:
  - Business continuity, operational resilience, and operational risk.

  - Ability to:
    - comply with legal and regulatory requirements;
    - conduct appropriate audits of the relevant function, service, or third party; and
    - identify, monitor, and manage all risks.
  - Obligations under:
    - the code; and
    - the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity of the institution or payment institution and its clients, including but not limited to UK GDPR and the Data Protection Act 2018.
- Participants, members, counterparties or customers and the wider ecosystem.
- Early intervention, recovery and resolution planning resolvability.
- The RPSO's or SSP's ability to scale up the outsourced service.
- Ability to substitute the third party or bring the outsourced service back in-house, including estimated costs, operational impact, risks and timeframe of an exit in stressed and non-stressed scenarios.

Notification to the Bank

5.10 Rule 2 of Part 4 of the Code of Practice (Notifications and Regulatory Reporting)] requires RPSOs and SSPs ~~are required~~ to notify the Bank in writing prior to entering into any new outsourcing agreement.~~,~~ Where an RPSO or SSP enters into, or significantly changes, a material third party arrangement it must submit such notifications using the template and following the guidance specified in Appendix 9. The data being collected aligns with the information outlined in Table C.

5.10A RPSOs and SSPs are ~~and is~~ expected to seek the Bank's non-objection when entering, or significantly changing a material ~~critical~~ outsourcing or third-party arrangement. Where a SSP providing services to a RPSO enters, or significantly changes a material ~~critical~~ outsourcing or third-party arrangement, the Bank also expects the RPSO to notify the Bank and seek the Bank's non-objection.

5.10B The Bank expects these notifications to be made before entering into the material ~~critical~~ outsourcing or third-party arrangement. The Bank also expects RPSOs and SSPs to submit these notifications before an outsourcing arrangement that was not initially deemed material ~~critical~~ is expected or planned to become so.

5.11 RPSOs, as risk managers within payment systems, are also expected to notify the Bank and seek the Bank's non-objection when there is a material change in their risk profile, and that of the end-to-end flow of payments across the payment system. This may include allowing participants to outsource their connectivity to the financial market infrastructure to the cloud.

5.12 RPSOs and SSPs should engage with the Bank early to confirm whether a proposed change falls within the scope of materiality ~~criticality~~, and if so, to discuss the information that the Bank will require in each case. The Bank expects information to be submitted sufficiently in advance of concluding any relevant contractual arrangement with the third party to allow time for the Bank to review the RPSO's or SSPs' proposal in principle, and for the RPSO or SPP to:

- provide additional information if requested to do so; and
- in the case of a planned outsourcing arrangement, to implement follow-up action if appropriate, which may involve:
  - enhancing its due diligence, governance, or risk management, and delaying entering into the agreement until it does so; or
  - reviewing the written agreement to ensure it complies with its regulatory obligations and risk management expectations (see Chapter 6). In some circumstances, it might be appropriate to notify the Bank sufficiently in advance before a final provider has been selected. An example of this is where a RPSO is planning a major migration programme and is still in the process of selecting a provider from a shortlist;
  - in the case where a RPSO has an existing outsourcing agreement with an SSP, to co-ordinate with the SSP to ensure that risks arising from interdependencies between all parties are understood and managed; and
  - in the case of participants' outsourcing arrangements, to implement follow-up actions, if appropriate, which may include:
    - enhancing its scheme rules;
    - setting out expectations that participants must meet to manage associated risks arising from their outsourcing arrangement; and
    - requiring participants to provide assurance of the resiliency of the solution outsourced to third parties eg testing.

Due diligence

5.13 The Bank expects RPSOs and SSPs to conduct appropriate due diligence on potential third parties before entering into an outsourcing or third-party arrangement, and to identify a suitable alternative or back-up provider(s) where available. Where relevant, RPSOs and SSPs should consider appropriate business continuity, contingency planning, and disaster recovery arrangements to ensure third parties can recover their support for the relevant important business service within their impact tolerances in the event of extreme but plausible disruption (see Chapter 10). RPSOs' and SSPs' due diligence should consider conflicts of interest in conformity with their conflicts of interest policy (see Paragraph 4.15).

5.14 The Bank expects RPSOs' and SSPs' due diligence to take into account expectations set out in Annex F, and furthermore to consider the potential providers':

- business model, complexity, financial situation, ownership structure, and scale;
- capability, expertise, and reputation;
- financial, human, and technology resources; and
- sub-outsourced third parties, if any, that will be involved in the delivery of important business services or parts thereof.

5.15 The due diligence should also consider whether potential third parties:

- have the appropriate authorisations or registrations required to perform the service;
- comply with UK GDPR, the Data Protection Act 2018, and other applicable legal and regulatory requirements on data protection;
- can demonstrate certified adherence to recognised, relevant industry standards;
- can provide, where applicable and upon request, relevant certificates and documentation (eg data dictionaries); and
- have the ability and capacity to provide the service that the RPSO or SSP needs in a manner compliant with UK regulatory requirements (including in the event of a sudden spike in demand for the relevant service, for instance as a result of a shift to remote working during a pandemic). A general track-record of previous performance may not be sufficient evidence by itself.

Risk assessment

5.16 In line with PFMI Principle 17 for Operational Risk, RPSOs should, in a proportionate manner, identify the plausible sources of operational risks. Consistent with Annex F, SSPs are also expected to identify and manage relevant operational and financial risks to its material ~~critical~~ services and ensure that its risk management processes are effective. These should include the potential risks arising from dependencies on third parties, regardless of criticality, and mitigate their impact through the use of appropriate systems, policies, procedures and controls. RPSOs and SSPs should also conduct risk analysis to identify how various scenarios affect the continuity of its important business services. The Bank expects RPSOs and SSPs to consider:

- operational risks based on an analysis of extreme but plausible scenarios and relevant output from a RPSO's or SSP's risk and control self-assessment and tail risk management process; for instance, a breach or outage affecting the confidentiality and integrity of sensitive data and/or availability of service provision;
- systemic risks posed by material ~~critical~~ third parties because one or more third parties are unable to meet their service obligations, thereby disrupting the important business

services of RPSOs or SSPs and affecting the financial stability of the wider UK economy; and
- financial risks, including the scenario where the RPSOs or SSPs are required to provide financial support to a material ~~critical~~ outsourced or sub-outsourced third party in distress or take over its business, including as a result of an economic downturn.

5.17 The Bank expects RPSOs and SSPs to carry out risk assessments when there is a significant change to an outsourcing arrangement's risks due to, for instance, a serious breach/continued breaches of the agreement or a crystallised risk or any other factors.

5.18 RPSOs' and SSPs' risk assessments should balance any risks that the third party or outsourcing arrangement may create against any other risks it may reduce. The assessment should also take into account the design and operating effectiveness of new, or existing, risk mitigation controls to ensure such arrangements remain within a RPSO's or SSP's risk appetite or threshold.

Concentration risk

5.19 As risk managers, the Bank expects RPSOs or SSPs to periodically (re)assess and take reasonable steps to identify and manage:

- their overall reliance on third parties; and
- concentration risks or vendor lock-in at the RPSO or SSP, due to:
  - multiple arrangements with the same or closely connected third parties;
  - sub-outsourcing or supply chain dependencies, for instance, where multiple otherwise unconnected third parties depend on the same sub-contractor for the delivery of their services;
  - arrangements with third parties that are difficult or impossible to substitute;
  - concentration of outsourcing and other third-party dependencies in a close geographical location, such as one jurisdiction. This type of concentration may arise even if a RPSO or SSP uses multiple, unconnected third parties, for instance, a business process outsourcing or offshoring hub; and
  - an indirect reliance on other third parties when participants outsource their financial market infrastructure connectivity, including hardware and other solutions, to the cloud. When multiple participants use common third parties, operational risks can be correspondingly concentrated, and the third party may become a source of systemic risk.

6: Outsourcing agreements

6.1 The outsourcing and third party risk management part of the code requires a formalised contractual agreement to be in place for all outsourcing arrangements, irrespective of materiality ~~criticality~~ and including intragroup arrangements.

6.2 Where there is a master service agreement that allows RPSOs or SSPs to add or remove certain services, each outsourced service should be appropriately documented, although not necessarily in a separate agreement.

6.3 RPSOs and SSPs should ensure that written agreements for all outsourcing arrangements include appropriate contractual safeguards to manage and monitor relevant risks. Moreover, regardless of materiality ~~criticality~~, RPSOs and SSPs should ensure that outsourcing arrangements do not impede or limit the Bank's ability to effectivity supervise the RPSO or SSP, or the outsourced activity, function or service.

Material ~~Critical~~ outsourcing agreements

6.4 Written agreements for material ~~critical~~ outsourcing arrangements should set out at least the following:

- a clear description of the outsourced function, including the type of support services to be provided;
- the extent to which the provision of each important business service of the RPSO or the SSP is dependent on a third party;
- the start date, next renewal date, end date, and notice periods regarding termination for the third party and the RPSO or SSP;
- the governing law of the agreement;
- the parties' financial obligations;
- whether the sub-outsourcing of a function or part thereof is permitted and, if so, under which conditions;
- the location(s), ie regions or countries, where the function or service will be provided, and/or where relevant data will be kept, processed, or transferred, including the possible storage location, and a requirement for the third party to give reasonable notice to the RPSO or SSP in advance, if it proposes to change said location(s);
- provisions regarding the accessibility, availability, integrity, confidentiality, privacy, and safety of relevant data (see Chapter 7);
- the right of the RPSO or SSP to monitor the third-party's performance on an ongoing basis (this may be by reference to key performance indicators (KPIs));

- the 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;
- the reporting obligations of the third party to the RPSO or SSP, including a requirement to notify the RPSO or SSP of any development that may have a material or adverse impact on the third party's ability to effectively perform the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements;
- whether the third party should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;
- the requirements for both parties to implement and test business contingency plans. For RPSOs and SSPs, these should take account of their impact tolerances for important business services as well as their recovery time and recovery point objectives. Both parties should commit to take reasonable, proportionate steps to develop an effective business continuity plan, and support the testing of such plans;
- provisions to ensure that data owned by the RPSO or SSP can be accessed promptly in the case of the insolvency, resolution, or discontinuation of business operations of the third party;
- the obligation of the third party to co-operate with the Bank, including persons appointed to act on their behalf;
- the rights of RPSOs or SSPs, and the Bank to inspect and audit the third party with regard to the outsourced function;
- if relevant:
  - appropriate and proportionate information security related objectives and measures, including requirements such as minimum information technology security requirements, specifications of RPSOs' or SSPs' data lifecycles, and any requirements regarding data security, network security, and security monitoring processes;
  - operational and security incident handling procedures, including escalation and reporting; and
  - termination rights and exit strategies covering both stressed and non-stressed scenarios, as specified in Chapter 10. As in the case of business contingency plans, both parties should commit to take reasonable steps to support the testing of RPSOs' or SSPs' termination plans. RPSOs and SSPs 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 appetite or tolerance; or
    - those that are not adequately notified and remediated in a timely manner.

6.5 If a third party in a material ~~critical~~ outsourcing arrangement is unable or unwilling to contractually facilitate a RPSO's or SSP's compliance with its regulatory obligations and expectations, the RPSO and SSPs should notify the Bank. The Bank will have due regard to a RPSO's or SSP's ability to fulfil its regulatory obligations. If an RPSO or SSP is unable to meet these obligations, the Bank may choose to issue a direction under Section 191 of the Banking Act in relation to the RPSO’s or SSP’s relationship with the third party.

7: Data security

7.1 In this chapter, the term data is defined broadly to include confidential, firm sensitive, and transactional data. It may also cover open source data (eg from social media) collected, analysed, and transferred for the purposes of providing financial services as well as the systems used to process, transfer, or store data. Where a third-party arrangement involves a transfer of data to the third party, irrespective of its materiality ~~criticality~~, or whether it relates to outsourcing or non-outsourcing, the Bank expects RPSOs and SSPs to have sound and robust information security policies, standards, and practices, and take appropriate measures to protect their data from unauthorised disclosure, ensure data integrity, and guarantee the availability of their services. This is in line with Annex F: Information Security. This chapter should also be interpreted consistently with requirements under relevant data protection law.

7.2 The expectations and requirements in this chapter apply to material ~~critical~~ outsourcing or third-party arrangments ~~agreements~~ that involve the transfer of data with third parties. Where a material ~~critical~~ outsourcing or third-party arrangments ~~agreement~~ involves the transfer of or access to data, the Bank expects RPSOs and SSPs to define, document, and understand their and the third parties' respective responsibilities in respect of that data and take appropriate measures to protect them.

7.3 Where a material ~~critical~~ outsourcing or third-party agreement involves the transfer of data, the Bank expects RPSOs and SSPs to:

- classify relevant data based on their confidentiality and sensitivity;
- identify potential risks relating to the relevant data and their impact (legal, reputational, etc);
- agree an appropriate level of data availability, confidentiality, and integrity;
- agree an appropriate recovery point and recovery time objective; and
- if appropriate, obtain appropriate assurance and documentation from third parties on the provenance or lineage of the data to satisfy themselves that it has been collected and processed in line with applicable legal and regulatory requirements.

7.4 Some risks relating to data that the Bank expects RPSOs and SSPs to consider include but are not necessarily limited to unauthorised access, loss, unavailability, and theft.

Data classification

7.5 RPSOs and SSPs are responsible for classifying their data. While the Bank does not prescribe a specific taxonomy for data classification, it expects RPSOs and SSPs to implement appropriate, risk-based technical and organisational measures, aligned to their broader operational risk framework, to protect different classes of data (eg confidential, client, personal, sensitive, transaction), when:

- developing and implementing their third party and outsourcing policy and other relevant policies and strategies, for example, business continuity planning, disaster recovery, information security, operational resilience, and risk management; and
- sharing data with third parties, including but not limited to, as part of an outsourcing arrangement.

Data location

7.6 The Bank recognises the potential benefits for operational resilience of RPSOs and SSPs using cloud technology to distribute their data and applications across multiple, geographically dispersed availability zones and regions. This approach can strengthen RPSOs' or SSPs' ability to respond to and recover from local operational outages faster and more effectively, and enhance their ability to cope with fluctuations in demand.

7.7 The Bank also recognises the potential negative consequences of restrictive data localisation requirements on RPSOs' and SSPs' innovation, resilience, and costs. None of the expectations in this SS and in particular this section should be interpreted as explicitly or implicitly favouring restrictive data localisation requirements.

7.8 However, the Bank expects RPSOs and SSPs to adopt a risk-based approach to the location of data that allows them to simultaneously leverage the operational resilience advantages of outsourced data being stored in multiple locations and manage relevant risks, which may include:

- legal risks stemming from conflicting or less developed relevant legal or regulatory requirements in one or more of the countries where the data may be processed or stored;
- challenges to RPSO's or SSP's and the Bank's ability to access data in a timely manner if required (eg as part of the Bank's enforcement, or supervisory functions) due to local law enforcement, legal, or political circumstances; and
- other potential risks to the availability, security, or confidentiality of data, for instance, high risk of unauthorised access or IT risks stemming from inadequate data processing equipment.

7.9 As part of their due diligence and risk assessment in the pre-outsourcing phase, RPSOs and SSPs should identify whether their data could be processed in any jurisdictions that are outside their risk appetite or tolerance and, if so, bring this to the attention of the third party when negotiating the contractual arrangement in order to discuss adequate data protection and risk mitigation measures.

Data security

7.10 The Bank expects RPSOs and SSPs to implement appropriate measures to protect any transfer of data to a third-party and set them out in their outsourcing and third-party risk management policy and, where appropriate, in their written agreements.

7.11 The Bank expects RPSOs and SSPs to leverage their existing risk governance and operational risk framework to assess the risks arising when data is in transit, in memory and at rest. RPSOs and SSPs should implement effective controls to mitigate the risks to within its risk appetite or tolerance. Depending on the materiality ~~criticality~~ and risk of the arrangement, these controls may include a range of preventative and detective measures, including but not necessarily limited to:

- configuration management. This is a particularly important measure, as for example, in the context of cloud, misconfiguration of cloud services can be a major cause of data breaches;
- encryption and key management;
- identity and access management, which should include stricter controls for individuals whose role can create a higher risk in the event of unauthorised access (eg systems administrators). RPSOs and SSPs should be particularly vigilant about privileged accounts becoming compromised as a result of phishing attacks and other leaking or theft of credentials;
- the ongoing monitoring of ‘insider threats’ (ie employees or agents of the RPSO or SSP, and at the third party who may misuse their legitimate access to enterprise data for unauthorised purposes maliciously or inadvertently). The term ‘employee’ should be construed broadly for these purposes and may include contractors, secondees, and sub-outsourced third parties;
- access and activity logging;
- incident detection and response;
- loss prevention and recovery;
- data segregation (if using a multi-tenant environment);
- operating system, network, and firewall configuration;
- staff training;
- the ongoing monitoring of the effectiveness of the third party’s controls, including through the exercise of access and audit rights (see Chapter 8);
- policies and procedures to detect activities that may impact RPSOs’ or SSPs’ information security (eg data breaches, incidents, or misuse of access by third parties) and respond to these incidents appropriately (including appropriate mechanisms for investigation and evidence collection after an incident); and
- procedures for the deletion of enterprise data from all the locations where the third party may have stored it following an exit or termination, provided that access to the data by the

RPSOs or SSP, or the Bank is no longer required. When deciding when to delete data, RPSOs and SSPs will need to consider their obligations under data protection law and their potential data retention obligations.

7.12 Where data is encrypted, RPSOs and SSPs should ensure that any encryption keys or other forms of protection are kept secure, by either the RPSO or SSP, or the outsourcing provider. The data protected by encryption (although not necessarily the encryption keys themselves) should be provided to the Bank in an accessible format if required.

7.13 The ability of third parties to respond to customer-specific data security requests may vary depending on the service being provided. Generally, the more standardised the service, the more difficult it might be for the third party to accommodate these requests. The Bank's focus is on the overall effectiveness of the third-party's security environment, which should allow RPSOs and SSPs to meet their regulatory and risk management obligations and be at least as effective as their in-house security environment. As long as third parties can provide assurance that this is the case, the Bank does not have specific expectations around customer-specific requests.

8: Access, audit and information rights

8.1 Section 204 of the Banking Act 2009 gives the Bank powers to request information that it requires in connection with its functions under the Act. These powers are not limited to RPSOs and SSPs and may apply directly to outsourced third parties to provide information which the Bank requires in pursuance of its financial stability objective.

8.2 The expectations and requirements in this chapter apply to critical outsourcing arrangements. However, the Bank expects RPSOs and SSPs to adopt a risk-based approach to access, audit, and information rights in respect of outsourcing arrangements with all third parties. In doing so, they should take into account the arrangement's riskiness and the likelihood of it becoming critical in the future.

8.3 The Bank requires a formalised contractual agreement to be in place for all outsourcing arrangements, irrespective of materiality ~~criticality~~ and including intragroup arrangements. The agreement should allow the RPSO, SSP and the Bank to have full access to such information it may require. The Bank expects RPSOs and SSPs to ensure that written agreements for material ~~critical~~ outsourcing arrangements include provisions for full access and unrestricted rights for audit and information to the following, so as to enable RPSOs and SSPs to comply with their legal and regulatory obligations, and to monitor the arrangement:

- the RPSO or SSP;
- the RPSO's and SSP's auditors;
- the Bank; and
- any other person appointed by the RPSO, SSP or the Bank.

8.4 RPSO's and SSP's proposals on effective access, audit and information rights should cover (as appropriate) premises, data, devices, information, systems and networks used for providing the service or monitoring its performance. These should include, where relevant:

- the third-party's policies, processes, and controls on data ethics, data governance, and data security;
- a summary of the results of security penetration testing carried out by the outsourced third party, 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 third-party's external auditors, personnel, and premises.

8.5 The Bank considers that it is not sufficient for RPSOs and SSPs merely to negotiate adequate access, audit, and information rights; these must also be used when appropriate. The purpose of the rights outlined in this chapter is to support RPSOs' or SSPs' identification, assessment, management, and mitigation of any identified risks relating to a material ~~critical~~

outsourcing arrangement. The appropriate exercise of these rights is key to providing the assurance that such an arrangement is being provided as agreed with the outsourced provider and in line with regulatory requirements. For example, assessing whether the third party is providing the relevant service effectively and in compliance with the RPSO's or SSP's regulatory obligations and expectations on operational resilience.

Pooled audits and third-party certificates and reports

8.6 RPSOs and SSPs may use a range of audit and other information gathering methods, including:

- offsite audits, such as certificates and other independent reports supplied by third parties; and
- onsite audits, either individually or in conjunction with other firms (pooled audits).

8.7 RPSOs and SSPs can choose any appropriate audit method as long as it enables them to meet their legal, regulatory, operational resilience, and risk management obligations. The level of assurance expected will, however become more onerous depending on the criticality of the arrangement. For instance, a RPSO that outsources an important business service for which it has set a low impact tolerance should demand a higher level of assurance.

Third-party reports and certificates

8.8 Certificates and reports supplied by third parties may help RPSOs and SSPs obtain assurance on the effectiveness of the third-party's controls. However, in outsourcing arrangements with material ~~critical~~ third parties, the Bank expects RPSOs and SSPs to:

- assess the adequacy of the information in these certificates and reports, and not assume that their mere existence or provision is sufficient evidence that the service is being provided in accordance with their legal, regulatory, and risk management obligations; and
- ensure that certificates and audit reports meet the expectations in Table D~~C~~.

Table D~~C~~: Expectations for certificates and audit reports

Component	Expectations
Scope	• Key systems and controls identified by the RPSO or SSP (eg applications, infrastructure, data centres, and processes). • Compliance with relevant requirements (eg the code).
Content	• Up-to-date information. • Reviewed regularly to reflect updates to the third-party's controls, new or revised legal, regulatory requirements, or expectations and recognised standards. • Where available, the Bank encourages the use of online, real-time reporting tools.
Expertise, qualification, and skills	• The auditing or certifying party and the person at the RPSO or SSP responsible for reviewing the certificate or report should have appropriate expertise, qualifications, and skills.
Process	• Test the effectiveness of the third-party's key systems and controls. • Performed in line with recognised standards.

8.9 In outsourcing arrangements with material ~~critical~~ third parties, the Bank expects RPSOs and SSPs to retain the contractual rights to:

- request additional, appropriate, and proportionate information if such a request is justified from legal, regulatory, or risk management perspectives; and
- perform onsite audits (individual or pooled) at their discretion.

Onsite audits

8.10 Before an onsite audit, the Bank expects RPSOs and SSPs, as well as individuals, and organisations acting on their behalf to:

- provide reasonable notice to the third party, unless this is not possible due to a crisis or emergency, or because it would defeat the purpose of the audit. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit;
- verify that whoever is performing the audit has appropriate expertise, qualifications, and skills; and

- take care, if undertaking an audit of a multi-tenanted environment (eg a cloud data centre), to avoid or mitigate risks to other clients of the third party in the course of the audit.

8.11 Certain types of onsite audit may create an unmanageable risk for the environment of the provider or its other clients, for example, by impacting service levels or the confidentiality, integrity, and availability of data. In such cases, the RPSO or SSP, and the third party may agree alternative ways to provide an equivalent level of assurance, for instance, through the inclusion of specific controls to be tested in a report or certification. The Bank expects that RPSOs and SSPs should retain their underlying right to conduct an onsite audit. For outsourcing arrangements with material ~~critical~~ third parties, the Bank would expect the RPSO or SSP to inform the Bank if alternative means of assurance have been agreed.

Pooled audits

8.12 Pooled audits may be organised by groups of firms sharing one or more third parties or facilitated by the third parties. They may be performed by representatives of the participating firms or specialists appointed on their behalf. Pooled audits can be more efficient and cost effective for RPSOs and SSPs and less disruptive for third parties running multi-tenanted environments. They can also help spread costs and disseminate best industry practices with regard to audit methods among RPSOs or SSPs.

8.13 Where pooled audits lead to common, shared findings, the Bank expects RPSOs and SSPs to assess what these findings mean for them individually, align risks and controls assessment to their broader operational risk framework and assess whether there are requirements for follow up actions or remediation on their part.

9: Sub-outsourcing

9.1 This section on sub-outsourcing builds on the existing PFMI Paragraph 3.17.20 where the contractual agreement for outsourcing should ensure that the RPSOs' approval is mandatory before the material ~~critical~~ third party or SSP can itself outsource critical elements of the service provided to the RPSO, and that in the event of such an arrangement, full access to the necessary information is preserved. This is also aligned to the expectation set out in Annex F: Risk identification and management. The expectations and requirements in this chapter apply to material ~~critical~~ outsourcing arrangements.

9.2 The Bank defines sub-outsourcing as a situation where the third party, or SSP, under an outsourcing arrangement further transfers, in whole or in part, an outsourced function to another third party. Sub-outsourcing, which is also sometimes referred to as 'chain' outsourcing, can amplify certain risks in an outsourcing arrangement, including:

- limiting RPSOs' or SSPs' ability to manage the risks of the outsourcing arrangement, in particular, where there are large chains of sub-outsourced third parties spread across multiple jurisdictions; and
- giving rise to additional or increased dependencies on certain third parties, which the RPSO or SSP may not be fully aware of or may not want.

Oversight of sub-outsourcing

9.3 The Bank expects RPSOs and SSPs to assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement. This includes any sub-outsourcing arrangements undertaken by a RPSO's SSP. It is important that RPSOs and SSPs have visibility of the dependencies arising from any chain outsourcing arrangements, and that third parties are encouraged to facilitate this by maintaining up-to-date lists of their sub-outsourced third parties.

9.4 The Bank expects RPSOs and SSPs to pay particular attention to the potential impact of large, complex sub-outsourcing chains on their operational resilience, including how this would affect their recovery time objectives, business continuity plans, and their ability to remain within impact tolerances during operational disruption. RPSOs and SSPs should also consider whether extensive sub-outsourcing could compromise their ability to manage their third-party risks by impairing their ability to oversee and monitor an outsourcing arrangement.

9.5 RPSOs and SSPs should assess whether each sub-outsourcing agreement meets the materiality ~~criticality~~ criteria set out in Chapter 5, which includes the potential impact on the RPSO's and SSP's operational resilience and the provision of important business services. RPSOs and SSPs should only agree to sub-outsourcing if:

- the sub-outsourcing will not impair the RPSO's or SSP's ability to manage its third-party risks;
- the risk assessment of such sub-outsourcing arrangement is within the RPSO's or SSP's risk appetite or tolerance;
- there is sufficient management information and reporting of key performance indicators, provided by the outsourced third party, or the sub-outsourcing third party that enables the RPSO or SSP to oversee and monitor the outsourced services; and
- sub-outsourced third parties undertake to:
    - comply with all applicable laws, regulatory requirements, and contractual obligations; and
    - grant the RPSO or SSP, and the Bank equivalent contractual access, audit, and information rights to those granted to the third party.

9.6 RPSOs and SSPs should ensure that the third party has the ability and capacity on an ongoing basis to appropriately oversee any material ~~critical~~ sub-outsourcing in line with the RPSO's or SSP's relevant policy or policies. This includes establishing that the third party has in place robust testing, monitoring, and control over its sub-outsourcing.

9.7 If the proposed sub-outsourcing could have significant adverse effects on an outsourcing arrangement to a material ~~critical~~ third party or would lead to a substantive increase of risk, the RPSO or SSP should exercise its right to object to the sub-outsourcing and/or terminate the contract.

9.8 There may be situations where the same third party has a direct contractual relationship with a RPSO or SSP, and is also a sub-outsourced third party to that RPSO or SSP. An example might be a RPSO that has an agreement with a CSP that provides services to one or more software vendors used by that third party firm. In those situations, where appropriate, RPSOs may leverage their direct contractual relationship with that third party to assess its resilience in respect of all the services it relies on that provider for, including as a critical sub-outsourced party.

Written agreement

9.9 In line with Chapter 6 on outsourcing agreements, the Bank expects written agreements for outsourcing to material ~~critical~~ third parties to indicate whether or not sub-outsourcing is permitted, and if so:

- define the materiality ~~criticality~~ of services and specify any activities that cannot be sub-outsourced;
- establish the conditions to be complied with in the case of permissible sub-outsourcing, including specifying that the third party is obliged to oversee those services that it has

sub-contracted to ensure that all contractual obligations between the third party and the RPSO and/or SSP are continuously met;

- require the third party to:
    - obtain prior specific or general written authorisation from the RPSO or SSP before transferring data (see Article 28 UK GDPR); and
    - inform the RPSO or SSP of any planned sub-outsourcing or material changes, in particular where that might affect the ability of the third party to meet its responsibilities under the outsourcing agreement. This includes planned significant changes to sub-contractors and to the notification period. RPSOs or SSP should be informed sufficiently early to allow them to at least carry out a risk assessment of the proposed changes and object to them before they come into effect; and
    - ensure that, where appropriate, RPSOs and SSPs have:
        - the right to explicitly approve or object to the intended sub-outsourcing or significant changes thereto; and
        - the contractual right to terminate the agreement in the case of specific circumstances (eg where the sub-outsourcing materially increases the risks for the RPSO or SSP, or where the third party sub-outsources without notifying the RPSO or SSP).

9.10 Below are some non-exhaustive examples of situations where a RPSO or SSP may consider exercising its contractual right to terminate the outsourcing agreement:

- without notifying the RPSO or SSP, the outsourced third party changed its list of sub-outsourced providers to include a firm that had a significant history of data breaches and operational outages;
- a sub-outsourced provider has failed to grant the RPSO or SSP, and/or the Bank, equivalent access, audit, and information rights;
- a significant incident at a sub-outsourced provider caused extensive and unmanageable operational disruption to a RPSO or SSP, so that it could no longer stay within its impact tolerances for important business services;
- a sub-outsourced provider repeatedly causes the outsourced provider to fail to meet KPIs and service expectations that have been agreed with the RPSO or SSP;
- a sub-outsourced provider enters into insolvency proceedings or other legal proceedings that may materially impact the delivery of its services; and
- actions taken following an incident fail to deliver appropriate remediation.

10: Business continuity and exit plans

10.1 The Bank's primary focus when it comes to business continuity plans and exit strategies is on the ability of RPSOs and SSPs to deliver important business services provided or supported by third parties in line with their impact tolerances in the event of extreme but plausible disruption. This is a requirement set out in the operational resilience part of the code, Paragraph 5 on scenario testing.

10.2 The expectations in this chapter apply to material ~~critical~~ outsourcing arrangements. Where a RPSO or SSP deems a non-outsourcing third-party arrangement as critical, it should implement appropriate and proportionate business continuity policies, procedures, and devote sufficient resources to ensure that its important business services are available, reliable and resilient.

10.3 For each material ~~critical~~ outsourcing arrangement, the Bank expects RPSOs and SSPs to develop, maintain, and test their business continuity plans; and amongst different scenarios, consider the following:

- a documented exit strategy, which should cover and differentiate between situations where a RPSO or SSP exits an outsourcing agreement:
    - in a stressed scenario, (eg following the failure or insolvency of the third party (stressed exit)); and
    - through a planned and managed exit due to commercial, performance, or strategic reasons (non-stressed exit).

10.4 The Bank recognises that in an intragroup outsourcing context, RPSOs' and SSPs' business continuity planning and exit options might be more limited than in other scenarios. In this context, the Bank expects RPSOs and SSPs to take reasonable steps to try and identify options, however limited, to maintain their operational resilience.

10.5 Notwithstanding the importance of effectively planning for non-stressed exits, the main focus of this chapter is on business continuity and stressed exits.

Business continuity

10.6 RPSOs and SSPs should implement appropriate business continuity plans for all material ~~critical~~ outsourcing arrangements to anticipate, withstand, respond to, and recover from extreme but plausible operational disruption. This is in line with PFMI Paragraph 3.17.14, where the objectives of an FMI business continuity plan should include the system's recovery time and recovery point. A RPSO's business continuity plan should ensure that it is able to resume operations within two hours following disruptive events, and the plan should be designed to enable the RPSO to complete settlement by the end of day even in the case of extreme circumstances. This is also in line with Annex F, where an SSP is expected to implement appropriate policies and procedures, and devote sufficient resources to ensure that its critical services are available, reliable, and resilient. Its business continuity management and disaster recovery plans should therefore support the timely resumption of its critical services in the event of an outage, so that the service provided fulfils the terms of its agreement with an RPSO. A SSP should have robust operations that meet or exceed the needs of the RPSO.

10.7 An important objective of the access, audit, and information rights in Chapter 8 is to enable RPSOs or SSPs, and the Bank to assess the effectiveness of third-parties' business continuity plans. In particular, they should be able to assess the extent to which, in the event of an extreme but plausible disruption scenario affecting the delivery of important business services for which a RPSO or SSP relies (wholly or in part) on the third party, such services can be recovered within the set impact tolerance. Where the IT services are outsourced, RPSOs and SSPs should further assess if the business continuity plan includes recovery time, and recovery point objectives, and plans to resume operations within two hours following disruptive events, and in the case of extreme circumstances, to complete settlement by the end of day.

10.8 For material ~~critical~~ cloud outsourcing arrangements, the Bank expects RPSOs and SSPs to assess the resilience requirements, including recovery time and recovery point objectives, of the service and data that are being outsourced and, with a risk-based approach, decide on one or more available cloud resiliency options. These may include:

- multiple data centres spread across geographical regions;
- multiple active data centres in different availability zones within the same region, which allows the third party to re-route services if a data centre goes down;
- a hybrid cloud (ie a combination of on-premise and public cloud data centres);
- multiple or back-up vendors;
- retaining the ability to bring data or applications back on-premise; and/or
- any other viable approach that can achieve and promote an appropriate level of resiliency.

10.9 There is no hierarchy or one-size-fits-all combination of cloud resiliency options. The optimal option or combination of options will depend on various factors, including but not limited to:

- size and internal organisation and the nature, scope, and complexity of the RPSO or SSP activities (proportionality);
- potential impact of the outsourcing arrangement on the provision of important business services by the RPSO or SSP (materiality ~~criticality~~); and

- the relative cost and benefits of different options, taking into account the risks that failure or prolonged operational disruption could ~~may~~ pose to UK financial stability.

10.10 If a RPSO or SSP wants to outsource its core payments platform to the cloud, or any part of the process, technology, facilities, and information required to deliver its important business service, the Bank may expect it to adopt one or more of the most resilient options available to maximise the chances of maintaining its resilience in the event of a serious outage. Conversely, if a RPSO or SSP wishes to outsource a business service that is classified as ‘not-important’, it may adopt a less resilient but nonetheless robust option or combination of options by adopting a proportionate and risk-based approach.

10.11 The Bank expects RPSOs and SSPs to consider the implications of deliberately destructive cyber attacks when establishing or reviewing data recovery capabilities, either individually or collaboratively with third parties.

10.12 In line with PFMI Paragraph 3.17.16, in the event of a disruption or emergency (including at a third party), RPSOs and SSPs should ensure that they have effective crisis communication measures in place. This is so all relevant internal and external stakeholders, including the Bank, PRA, FCA, other international regulators, and, if relevant, the third-parties themselves, are informed in a timely and appropriate manner. This is also consistent with Annex F where SSP should have effective customer communication procedures and processes. In particular, SSPs should provide the RPSO and, where appropriate, its participants with sufficient information so that users clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided.

Stress exit scenario

10.13 RPSOs’ and SSPs’ exit plans should cover stressed exits and be appropriately documented and tested as far as possible.

10.14 A key objective of the stressed exit part of exit plans is to provide a last resort risk mitigation strategy in the event of disruption that cannot be managed through other business continuity measures, including those mentioned in the previous section (eg the insolvency or liquidation of a third party).

10.15 The Bank does not prescribe or have a preferred form of exit in stressed scenarios. Its focus is on the outcome of the exit that supports financial stability (ie the continued provision by the RPSO or SSP of important business services provided or supported by third parties), rather than the method by which it is achieved.

10.16 The Bank does, however, expect RPSOs and SSPs to identify viable forms of exit in a stressed exit scenario, and give meaningful consideration to those that best safeguard their operational resilience, which may include but not be limited to:

- bringing the data, function, or service back in-house/on-premise;
- transferring the data, function, or service to an alternative or back-up third party; or
- any other viable methods.

10.17 The Bank expects RPSOs and SSPs to consider the available tools that could help facilitate an orderly stressed exit from a material ~~critical~~ outsourcing arrangement. Such tools are constantly evolving, in particular in technology outsourcing, including cloud, and may include, but are not limited to:

- new potential third parties;
- technology solutions and tools to facilitate the switching and portability of data and applications; and
- industry codes and standards.

10.18 RPSOs and SSPs should also actively consider temporary measures that can help ensure the ongoing provision of important business services following a disruption and/or a stressed exit, even if these are not suitable long-term solutions (eg contractual or escrow arrangements), allowing for continued use of a service or technology for a transitional period following termination.

Governance of business continuity and exit plans

10.19 RPSOs and SSPs should begin to develop their business continuity and exit plans, in particular for stressed exits, during the pre-outsourcing phase once they have determined that a planned outsourcing arrangement is classified as critical. Doing so will enable them to:

- use the due diligence process to identify potential alternative or back-up third parties;
- estimate the cost, resourcing, and timing implications of the proposed business continuity or exit plan in both stressed and non-stressed scenarios as part of the risk assessment;
- identify data they may need to access, recover, or transfer as a priority in a disruption or stressed exit;
- define the KPIs and key risk indicators which, if breached, may trigger an exit (both stressed and non-stressed); and
- assess the operational risk of the business continuity and exit plans to ensure that the plans do not introduce significant incremental risks and that the overall operational risk remains within existing board approved risk appetite.

10.20 RPSOs and SSPs should evaluate what would be involved in delivering an effective stressed exit and use this to formulate plans for such an exit, assisting them in identifying any assets and skills required. As soon as practically possible, RPSOs and SSPs should seek to test the stressed exit plans to ensure they are functional and meet expectations around service continuity, impact tolerances and costs etc.

10.21 Once an outsourcing arrangement has been implemented, RPSOs and SSPs should test their business continuity and exit plans using a risk-based approach. Where possible and relevant, this testing should align to, support, or even be a component of the RPSO's or SSP's scenario testing in meeting UK regulatory operational resilience policy expectations. For instance, the extreme but plausible scenarios that a RPSO or SSP may select for testing could involve: a failure or disruption at a third party or their supply chain, or a cyber attack at the third party, resulting in breaches of confidential data. RPSOs and SSPs should have due regard to previous incidents or near misses within the organisation, across the financial sector and in other sectors and jurisdictions, as well as business and system disruption scenarios developed for the management of tail risks or capital setting, where applicable.

10.22 For RPSOs and SSPs that are subject to the **CBEST framework**, the CBEST implementation guide notes that 'Malicious Insider and Supply Chain Scenarios are a feature of the threat landscape for many firms. These scenarios should always be analysed and discussed during CBEST'. Where required, RPSOs and SSPs 'should plan in advance the involvement of staff and third parties to increase the reality of assessment'.

10.23 Consistent with PFMI Paragraph 3.17.17, RPSOs should update their business continuity and exit plans with lessons learned from these tests, including with new risks and threats identified and changed recovery objectives and priorities (if any). This is also consistent with Annex F, where a SSP should have robust business continuity and disaster recovery objectives and plans. These plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption.

10.24 RPSOs and SSPs should assign clear roles and responsibilities for business continuity and exit plans. Subject to proportionality, they may establish cross-disciplinary teams to develop, document, test, and execute their business continuity and exit plans, especially in stressed scenarios (which should include communicating with the Bank and other relevant stakeholders in the event of disruption). These teams should include relevant business lines, control functions, technical experts (eg IT specialists), and be chaired by a member of the executive of the RPSO or SSP. RPSOs and SSPs should also allocate responsibility for signing off business continuity and exit plans, including updates thereafter, and the decision to activate them.

10.25 When developing business continuity and exit plans, RPSOs and SSPs should define the objectives of the plan, including what would constitute successful business continuity or a successful exit in both stressed and non-stressed scenarios, by reference to measurable criteria such as costs, functionality, time, and the RPSO's or SSP's impact tolerances for important business services. Where relevant, business continuity plans should have due regard to the recovery time objectives set out by PFMI Paragraph 3.17.14.

10.26 RPSOs and SSPs should take reasonable steps to test exit plans; in particular, those relating to stressed exits. The extent and nature of testing will vary depending on the type of outsourcing arrangement and corresponding exit plan. For instance, a RPSO running a hybrid cloud structure may take into account the potential back-up functions located in its private cloud elements. Likewise, a SSP that keeps backup copies of data which it has outsourced to the cloud may focus its testing on assessing the ongoing consistency of both sets of data and reconciling them as appropriate. RPSOs and SSPs should also assess and take reasonable steps to manage any operational risks that may be caused or increased by the actual testing (eg data theft).

10.27 Business continuity and exit plans should be reviewed, updated and tested periodically to ensure such plans are kept up to date and take into account triggers or developments that may change the feasibility of the business continuity measures or an exit. These triggers or developments may include those in the following non exhaustive list:

- the emergence of threats, or the identification of vulnerabilities;
- an increase in the number of availability zones or regions offered by a current third party;
- changes to the RPSO’s or SSP’s business requirements;
- the emergence of new, potentially viable alternative providers; and/or
- developments in technology or other tools to facilitate the porting of data and applications (eg among cloud providers or between RPSOs’ and SSPs’ on-premises environments and the cloud).