FSB FINANCIAL STABILITY BOARD

Guidance on Arrangements to Support Operational Continuity in Resolution

Revised version

18 March 2024

(*Supplementary note on digitalisation of critical shared services added to 2016 Guidance*)

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on X\Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Guidance on Arrangements to Support Operational Continuity in Resolution (2016)

1. Introduction

1.1. This Guidance should assist supervisory and resolution authorities and firms to evaluate whether firms that are subject to resolution planning requirements have appropriate arrangements to support operational continuity if the firm enters resolution. It supports the objectives of the *FSB Key Attributes of Effective Resolution Regimes for Financial Institutions ('Key Attributes'* or KAs*),*[1] which specify that resolution regimes should, among other things, ensure continuity of systemically important financial functions of a firm in resolution. In particular, it complements the guidance on resolution planning set out in I-Annex 3 (*Resolvability Assessments*) and I-Annex 4 (*Essential Elements of Recovery and Resolution Plans*) to the *Key Attributes*. It should also be read in conjunction with the FSB guidance on "Identification of Critical Functions and Critical Shared Services"[2] published in July 2013.

1.2. Operational continuity refers to the ability to continue critical shared services[3] that are necessary to maintain the provision or facilitate the orderly wind down of a firm's critical functions in resolution. Critical shared services and critical functions are intrinsically linked: without continuity of critical shared services, the continued provision of critical functions in resolution is unlikely to be possible. Operational continuity is therefore a key aspect of resolution planning for individual firms and a lack of adequate arrangements for operational continuity is likely to impair firms' resolvability.

1.3. The first round of the FSB Resolvability Assessment Process[4] ('RAP') found that a lack of adequate arrangements for operational continuity poses an obstacle to the orderly resolution of many of the Global systemically important banks ('G-SIBs') that were assessed.[5] Factors that may result in disruption or create uncertainty in relation to operational continuity include:

(i) firms' interconnectedness and complexity, including a lack of clear mapping between legal entities and business lines and the critical shared services that they rely upon;

(ii) insufficiently detailed contractual arrangements for intra-group and third-party service provision;

---

1 FSB (2014), *Key Attributes of Effective Resolution Regimes for Financial Institutions*, October.

2 FSB (2013), *Guidance on Identification of Critical Functions and Critical Shared Services*, July.

3 An activity, function or service performed by either an internal unit, a separate legal entity within the group or an external provider, performed for one or more business units or legal entities of the group, the failure of which would lead to the collapse of (or present a serious impediment to the performance of) critical functions.

4 The FSB Resolvability Assessment Process requires a discussion of the resolvability of each G-SIFI at senior level within the Crisis Management Group, a letter to the FSB Chair summarising the general findings and a resolvability report drawn up on the basis of the findings for all G-SIFIs.

5 FSB (2014), *Resolution Progress Report,* November.

(iii) contractual provisions that permit service providers to terminate services on the entry into resolution of the service recipient without requiring a failure to pay or other performance-related default; and

(iv) inability to provide timely and accurate information relating to critical shared services, including on the service recipients, the arrangements by which the services are provided, charging structures, ownership of assets and infrastructure associated with the services, and location of key staff; and uncertainty as to whether continuity can be secured where the services are provided by unregulated entities or service providers located in different jurisdictions.

1.4. This guidance identifies a number of arrangements including specific contractual provisions, access arrangements and governance structures that, if implemented appropriately, could support operational continuity in resolution. The guidance discusses those arrangements in the context of three service delivery models: (i) service provision within a regulated entity; (ii) service provision by an intra-group service company; and (iii) service provision by a third-party service provider. The guidance recognises that large firms are likely to use a combination of the three models. There is no presumption that firms, or certain types of firms, should adopt any particular model. The purpose of the guidance, rather, is to identify features and arrangements that are likely to reinforce the resilience of those models with a view to supporting continuity of the services provided in resolution.

1.5. The arrangements adopted to support operational continuity by global systemically important financial institutions ('G-SIFIs') and other firms for which resolution planning is required will be considered by authorities in resolvability assessments. Where authorities identify weaknesses in firms' arrangements that are considered to impair resolvability, they may exercise powers, including those specified in the *Key Attributes,* to require firms to modify those arrangements in order to improve their resolvability.[6] The FSB will continue to monitor and report on obstacles to resolvability, including those related to operational continuity, and the extent to which they are being addressed, in the RAP over the coming years.

1.6. The guidance does not specifically address continued access to Financial Market Infrastructure ('FMI') services. The FSB acknowledges that this may be essential to support continuity of certain critical functions and is considering this aspect separately.

[6] See KA 10.5, which specifies that supervisory authorities or resolution authorities should have powers to require the adoption of measures to improve resolvability.

2. The concept of operational continuity

Critical shared services and critical functions

2.1. Operational continuity refers to the means of ensuring or supporting continuity of the critical shared services that are necessary to maintain the provision or facilitate the orderly wind down of a firm's critical functions in resolution.

2.2. Operational continuity is defined in the context of critical functions and critical shared services.

- **Critical functions** are activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the size or market share of the financial institution or group, its external and internal interconnectedness, complexity and cross-border activities.

- **Critical shared services** are activities, functions or services performed for one or more business units or legal entities of the group, performed by either an internal unit, a separate legal entity within the group or an external provider, and the failure of which would lead to the collapse of (or present a serious impediment to the performance of) critical functions.

2.3. There are two main categories of critical shared services:

- **Finance-related shared services** involve the management of financial resources of the financial institution or group related to the operation or provision of critical function(s). This includes, but is not limited to: treasury-related services, trading, asset management, cash handling, risk management and valuation.

- **Operational shared services** provide the necessary infrastructure to enable the financial institution or group to operate or provide critical function(s). This includes, but is not limited to: IT infrastructure and software-related services; personnel and human resources support, procurement and facilities management; and transaction processing. Functions such as legal and compliance are also considered as operational shared services.

2.4. The arrangements to support operational continuity set out in this guidance focus primarily on the provision of shared services that are transactional, such as IT and certain operational functions, and can be addressed by contractual terms. The arrangements identified in this guidance would not be suitable for shared services that involve risk-taking or require strategic judgements, including certain parts of treasury or risk management functions.

2.5. Authorities should identify the critical functions and critical shared services of a particular firm as part of the resolution planning process. The FSB guidance on "Identification of Critical Functions and Critical Shared Services" sets out a process for determining critical shared services and critical functions and provides an indicative list

of shared services that could be regarded as critical, subject to certain conditions being met.

2.6. Operational continuity of critical shared services should be viewed as a key part of resolution planning and resolvability for individual firms.[7] This applies irrespective of the resolution strategy and the resolution tool(s) that may be used. Similarly, the arrangements to support operational continuity discussed in Section 4 below are equally relevant irrespective of the resolution strategy that is applied, although authorities will need to consider how the arrangements might need to be adapted to facilitate separation of parts of the group in the resolution transaction or post-stabilisation restructuring (see paragraphs 4.8 and 4.9).

Operational continuity as a going concern supervisory consideration

2.7. Although this guidance assesses operational continuity in resolution, operational continuity is also a going concern supervisory consideration. In most cases, going concern operational continuity is considered in the context of a firm's resilience and business continuity planning ('BCP'); that is, its ability to recover business operations in response to incidents such as IT failures, cyber-attacks, natural disasters and geo-political disruptions.

2.8. Going concern operational continuity is also considered in the context of outsourcing, where a firm contracts with a third party for the performance of a business process. A number of jurisdictions have issued supervisory rules or expectations in relation to outsourcing, in view of the operational risk that this creates.

2.9. There are some parallels between operational continuity for resolution and operational continuity for BCP and outsourcing, even if the triggers and frameworks are different. For example, BCP typically begins with an identification of critical processes that would need to be recovered in the event of business disruption. Although this is mainly based on the firm's own assessment of what functions and shared services are critical, there is likely to be substantial correlation with those that have been identified as critical for the purposes of resolution planning. However, it cannot be assumed that the functions and services will be identical and a separate analysis should be carried out for resolution purposes (see paragraphs 3.2 and 3.3 below).

2.10. There could also be tension between arrangements that support operational continuity in going concern and those that support operational continuity in resolution. For example, operating discrete IT systems in different regions or business areas could support restructuring or recovery options but, when compared to integrated firm-wide systems, may reduce efficiencies and create additional operational risk in a 'business as usual' context.

---

[7] The *Key Attributes* refer to the continuity of critical functions in the resolvability assessment (10.2(i), I-Annex 3) and the recovery and resolution plans (11.6(i), I-Annex 4).

2.11. Given these possible tensions and trade-offs, actions to improve the adequacy of arrangements for operational continuity in resolution should consider any risks and/or adverse impact such actions may have on a firm as a going concern.

3. Service delivery models and resolvability

3.1. This guidance distinguishes between three different service delivery models that firms typically adopt for the provision of operational services:

(i) provision of services by a division within a regulated legal entity;

(ii) provision of services by an intra-group service company; and

(iii) provision of services by a third-party service provider.

3.2. These three models are not mutually exclusive, and many firms employ a mixed service delivery model that combines different models. Resolution strategies and approaches to operational continuity will therefore have to take into account the different service models used across the group and how they interact. However, firms should also review their service delivery models from the perspective of resolvability to ensure that they are appropriate to specific shared services that will support critical functions in resolution. While the starting point of that work may be business continuity planning, additional analysis of resolution scenarios will also be needed, including expectations regarding post-stabilisation restructuring.

3.3. In particular, a more granular analysis of criticality of functions is likely to be needed for the purposes of resolution than for ordinary business continuity planning so that the services that support the highest priority functions can be identified. Irrespective of the service delivery model used, a comprehensive, regularly updated mapping between critical functions, shared services and legal entities (both those providing and those receiving critical services) will also be necessary to support resolution planning and execution.

3.4. It is important to note that although each model has specific strengths and weaknesses, examples of which are set out below, they should each be of sufficient strength if appropriately designed. The most suitable model (or combination of models) for an individual firm should be aligned with its business and operating model and be consistent with the applicable legal framework and regulatory standards.

Provision of services within a regulated legal entity

3.5. Under this model, operational services are provided ‘in-house’ from a regulated entity either to other entities in the group (“inter-entity”) or within the regulated entity itself (“intra-entity”, e.g. from the regulated entity to a foreign branch of the regulated entity).

3.6. In a going concern, housing operational services within a regulated entity may improve transparency, access and ease of supervision. In resolution, provided that the

resolution authority has relevant powers in relation to the regulated entity, it should be able to provide for the continued provision of critical shared services.

3.7. This model may create difficulties in the legal and operational separation of critical functions and uncertainty for service recipients based outside the jurisdiction of the regulated entity in resolution. These challenges can be addressed if services provided to other entities in the group are supported by adequate contractual documentation and transparent, arm's length pricing mechanisms. The model may also need to be supported by arrangements for the retention or substitution of key staff from business lines that may be wound down or disposed of in resolution, as well as continued access to intellectual property owned by the parent or other entities outside the regulated entity.

Provision of services by an intra-group service company

3.8. Under this model, operational services are provided to different group entities from a dedicated intra-group service company.

3.9. Services from an intra-group service company tend to be provided on the basis of intra-group service level agreements ('SLAs') and a defined fee charging mechanism. The intra-group service company will also typically own the assets (including intellectual property rights) and infrastructure required to run the services, and may have dedicated governing structures and management. To the extent that service provision under such arrangements is clearly documented, this is likely to facilitate mapping of services to recipient entities and provide greater clarity about which shared services need to continue in resolution. Such arrangements may also facilitate the restructuring of business lines or legal entities within the group as part of resolution.

3.10. However, even if intra-group SLAs are well defined, authorities should still consider the potential challenges for enforceability or continued performance of services that may arise. For example, a statutory power of resolution authorities to enforce SLAs or the continued performance of services may be challenging if the service company is not prudentially regulated unless the resolution regime gives the resolution authority powers over unregulated entities (and the entity is subject to the jurisdiction of the authority). Similarly, an 'off-shore' service company may be located in a jurisdiction where efforts of the home resolution authority to enforce continued provision of services under the SLA may not be supported by local authorities or courts.

3.11. The model may also need to be supported by arrangements to ensure intra-group service companies have sufficient financial resources to cover their own operating costs throughout resolution.

Provision of services by a third-party service provider

3.12. Under this structure, a firm outsources operational service(s) to an external service provider on a contractual basis. This could include the sub-contracting of operational services from a regulated entity or an intra-group service company.

3.13. A third-party service model tends to result in the most formalised contractual arrangements, which can provide greater clarity in resolution and may also provide flexibility in terms of scaling resources and services. The more diverse client base of many third-party service providers may also aid financial resilience, so that a provider's viability is less likely to be threatened by the entry into resolution of a client firm.

3.14. This structure may support restructuring of a group in resolution through divestments of legal entities or business lines, due to the flexibility it offers in the management of services and resources. However, that benefit will be diminished to the extent that the transfer of third-party service agreements as part of a restructuring is restricted, and must also be balanced against the likelihood that the resolution authority has limited or no powers over the third-party service provider to help ensure operational continuity in resolution. For example, the resolution authority may not be able to prevent the service provider from modifying the terms of the contract or exercising contractual rights (including cross-default rights) to terminate the provision of services on entry into resolution of the firm. As with other models, this risk could be addressed by the use of SLAs that provide for continuity of the covered services in resolution. In any event, this risk may be low if the service provider can be reasonably confident that it will continue to be paid.

3.15. Joint venture entities that are co-owned and controlled by two or more firms represent a particular version of third-party service provision. While such arrangements might bring benefits of cost efficiency during 'business as usual', they may also give rise to specific complications and risks if one of the parties to the joint venture fails or enters resolution. For example, the structure and governance of joint ventures may create challenges in determining who owns shared services assets and which business lines or legal entities those assets support. Particular attention may need to be given to planning for operational continuity in those circumstances.

4. Possible arrangements to support operational continuity

4.1. The development of appropriate operational continuity arrangements is likely to be an iterative process between resolution authorities and firms, and the effectiveness of a particular service model (or combination of models) in supporting operational continuity will need to be assessed on a firm-by-firm basis as part of the resolvability assessment. That assessment would depend on the provision of accurate and detailed information[8] and would be considered in light of the resolution strategy for the firm and against the various circumstances in which the firm might plausibly enter resolution.

4.2. The firm's service model needs to provide operational continuity in the two stages of resolution:

(i) stabilisation (the point at which resolution tools are applied); and

[8] Refer to the Annex for examples of the types of information that authorities may require.

(ii) wind-down and/or restructuring (the period in which the firm is wound down or restructured to create a viable business model, for example, by divesting or winding down legal entities or business lines), recognising that the exact restructuring needs will depend on, amongst other things, the circumstances that led to the firm's failure and market conditions at the time of resolution.

4.3. Thought should also be given in resolution planning about how to manage the transition from 'business as usual' to the operation of a firm in resolution.

4.4. To provide operational continuity in the two stages of resolution, the following arrangements could be considered. Most or all of the arrangements should be relevant for all of the service delivery models discussed above, although the way in which they are implemented will need to be adapted to the specific model in question.

(i) **Contractual provisions -** Firms should have clearly and comprehensively documented contractual arrangements and SLAs for both intra-group and third-party critical shared services which, to the greatest extent possible, remain valid and enforceable in resolution provided there is no default in payment obligations. This is discussed further under the following subsection on *'*Contractual provisions'.

(ii) **Management information systems ('MIS') -** All arrangements and models should be supported by a clear taxonomy of shared services and the maintenance of up-to date mapping of services to entities, businesses and critical functions. MIS should allow for timely reporting on the provision or receipt of critical shared services on a legal entity and line of business basis, including information about ownership of assets and infrastructure; pricing; contractual rights and agreements; and outsourcing arrangements.

(iii) **Financial resources -** Intra-group providers of critical shared services (including where the services are provided within regulated entities) should have sufficient financial resources to facilitate operational continuity of critical functions in resolution. Where an entity relies on third-party critical shared services, the service recipient should have sufficient financial resources to ensure that the third-party provider continues to be paid. In all cases, the financial resources should be sufficient to cover the stabilisation phase of resolution and to facilitate the subsequent restructuring period.[9] Communication with a third-party service provider as regards to continued payment can help manage the risks of early termination.

(iv) **Robust pricing structures -** Cost and pricing structures for services should, to the extent permitted by tax and legislative requirements, be predictable, transparent and set on an arm's length basis with clear links, where relevant, between the original direct cost of the service and the allocated cost. The cost

[9] Recognising that the resolution group (or resolution groups) may be 'right sized' during the restructuring phase, as parts of the business are sold or wound down, and that recapitalised entities may have access to sources of liquidity (see the FSB's Guiding principles on the temporary funding needed to support the orderly resolution of a G-SIB, [LINK].

structure for services should not alter solely as a result of the entry into resolution of the service recipient. This arrangement is relevant for the provision of critical shared services through an intra-group service company (to ensure the service company is financially viable on a standalone basis) or through a regulated entity (to ensure that the documentation could form the basis of an external contract if the regulated entity is restructured in resolution).

(v) **Operational resilience and resourcing -** Critical shared services should be operationally resilient and have sufficient capacity (for example, human resources and expertise) to support the restructuring phase following the failure of a group entity or group entities. Firms and authorities should plan for the retention of critical employees necessary for the provision of critical shared services in resolution. In any event, critical shared services should not be unduly affected by the failure or resolution of other group entities.

(vi) **Governance -** Critical shared services should have their own governance structure and clearly defined reporting lines. Where services are provided by a division of a regulated entity, for example, this could entail some element of independent management and responsibility at board level. Critical shared service providers should have sufficient governance oversight or planning and contingency arrangements to ensure that services continue to be provided in resolution without relying on senior staff from certain business lines that may be wound down or that may no longer form part of the same group. The governance arrangements relating to critical shared services could be assessed by the firm's internal audit function.

(vii) **Rights of use and access -** Access to operational assets by the critical shared services provider, the serviced entities, business units and authorities should not be disrupted by the failure or resolution of any particular group entity. In some cases, this may require that operational assets essential to the provision of critical shared services are owned or leased by the same legal entity providing those critical shared services (that is, by the regulated entity or by the intra-group service company, depending on the model used). Where this is not the case, contractual provisions to ensure rights of access could be considered. Service recipients should also not be restricted from using shared assets directly where appropriate. Continued access to IT, intellectual property and operational services during the restructuring period (for example, through Transitional Service Agreements, as discussed under 'Contractual provisions' below) should be considered as part of resolution planning.

4.5. In addition, firms should consider developing and maintaining an operational continuity 'playbook' that would describe the actions and steps in order to facilitate operational continuity following the entry of the firm into resolution.

Contractual provisions

4.6. Poorly designed or inadequate SLAs may represent a significant obstacle to operational continuity in resolution, and there is a risk that intra-group and third-party SLAs will be

terminated upon entry of a firm into resolution without any default in payment. These obstacles and risks can be mitigated by the following measures.

(i) Services received from both third-party and intra-group entities should be well documented and have clear parameters against which service provision can be measured. This should include details of the provider and recipient(s) of the service, the nature of service and its pricing structure. This should also include any onward provision to other entities or sub-contracting to third-party providers. For services provided by a division of a regulated entity, SLAs should be sufficiently granular to allow them to form the basis of effective Transitional Service Agreements to facilitate post resolution restructuring that may be required.

(ii) The terms of SLA service provision and pricing should not alter solely as a result of the entry into resolution of a party to the contract (or affiliate of a party). The resolution authority should be able to maintain the service contract on the same terms and conditions that were imposed prior to resolution for intra-group service contracts and, to the extent permitted under applicable law, third-party service contracts.

(iii) SLAs should explicitly contemplate that services may be transferred or assigned in resolution. As long as payments and other obligations continue to be met, the service provider should not have a right of termination by reason of any such assignment or transfer.

(iv) SLAs designed to provide service to a "group" should have clauses that as far as possible allow for the continued use of such products or receipt of such services by (former) group entities for a reasonable period of time following a divestment resulting from a resolution, in order to support group restructuring.

(v) In the absence of an explicit statutory provision that prevents contract termination or contractual modification solely on the grounds of early intervention or resolution, SLAs should include explicit provisions that achieve the same outcome, subject to adequate safeguards and continuity of performance under the contract.

4.7. Consistent with the Key Attributes, (KA 3.2 (iv)), resolution authorities should have powers to require local companies in the same group (whether or not regulated) within the jurisdiction to continue to provide services that are necessary to support continuity of essential services and functions to a firm in resolution.

Resolution strategies and post-stabilisation restructuring

4.8. A service model that facilitates business separability and restructuring will be particularly important for resolution strategies that involve the transfer of part of the business or a separation of legal entities at the point of resolution.

4.9. Any service model (or combination of models) used by a firm will need to support business separability and restructuring, even if the firm's resolution strategy aims to

keep the group largely intact. Even in the execution of an SPE strategy, it cannot be assumed that the structure and business operations of the firm will remain unchanged: restructuring is likely to be necessary to address the problem(s) that caused the firm to enter resolution, and non-material entities may not be preserved. Options for divestment should be contemplated under any resolution strategy, and this should be taken into account in planning for operational continuity. Moreover, the actual resolution will depend on the circumstances of the failure (even if authorities have developed preferred resolution strategies).

Cross-border provision of shared services

4.10. Ensuring operational continuity may be more difficult when services are provided by an entity outside of the jurisdiction of the resolution authority (or resolution authorities). There may be particular challenges in securing operational continuity with respect to foreign law governed arrangements and interacting with official sector counterparts in the jurisdiction of the service provider, where the entity in question may not be prudentially regulated. These challenges are outside the scope of this work and the guidance does not seek to directly address them.

4.11. Finally, in order to support cross-border cooperation in the execution of a resolution strategy, home authorities should as far as possible provide host authorities with reasonable comfort that in-house or intra-group service providers have sufficient financial resilience and appropriate governance arrangements, and will continue to provide critical shared services that support critical functions in the host jurisdiction. This may be particularly pertinent, for example, where critical shared services are provided to local subsidiaries from a branch in the host jurisdiction.

Annex: Indicative information requirements to facilitate operational continuity

This Annex provides guidance with respect to the types of information that could be available to support firms and resolution authorities in their assessment of operational continuity in resolution. The types and categories of information listed below are indicative and resolution authorities will need to adapt the information requirements to the specific service delivery model(s) employed by the firm, as each model (or combination of models) is likely to present its own challenges.

The general effectiveness of operational continuity planning is increased if the following conditions are met.

- **Accessibility:** the firm should have adequate MIS to allow timely access to complete and accurate information. Examples of these systems include but are not limited to: searchable centralised repositories for intra-group and third-party service contracts, software application catalogues, human resource databases and agreement repositories related to systems, facilities and intellectual property.

- **Mapping:** firms should identify legal entities and business lines or divisions that perform critical functions and the critical shared services they receive. There should be a clear mapping between critical shared service providers and recipients. This mapping should include relevant details such as the jurisdiction of each party; description of the service; and which of the service delivery models (as described above in Section 3) is being used. This mapping should also include services provided between critical shared service providers, if relevant (e.g. an intra-group service company sub-contracting with a third-party service provider).

The types and categories of information that could be required apply to both SPE and MPE resolution strategies. In addition, the information that could be required would be relevant to both the stabilisation and restructuring phases of resolution.

1. Information requirements: Staff required for the provision of critical shared services

a) Identification of staff (full time equivalents ('FTEs'), contract employees, other) or functions required for each critical service, distinguishing between FTEs or functions dedicated to support critical functions and FTEs or functions delivering group-wide services;

b) The firm's processes and procedures for identifying and retaining critical personnel;

c) Identification of the entity that employs staff that provide critical shared services. Where the entity is outside of the resolution group, information requirements will be similar to Annex Section 3 below for the SLAs that govern the provision of service; and

d) The firm's existing planning and contingency options for the unavailability of critical employees (e.g., ability to outsource). Such planning may already exist in business continuity plans or other documented processes.

2. Information requirements: Operational, legal and governance structure of critical shared services

2.1. A description of the operational, legal and governance structure of the service provider including, but not limited to:

a) Jurisdiction(s) where services are centralised;

b) Contracts governing the provision of services (see Annex Section 3 below for details), including a description of the pricing policies that govern the provision of services; and

c) Inventory, including location, of operational assets necessary to provide critical shared services.

2.2. For provision of services by an intra-group service company, analysis of actual and stressed financial condition of the service company(s) with a view to assessing the ability to continue providing services through resolution, along with supplemental information including, but not limited to:

a) Balance sheets, income statements and statement of cash flows;

b) Projected liquidity, capital and cash flows of the service company through stressed conditions such as the failure and entry into resolution of one or more group entities to which intra-group services are provided; and

c) Description of liquidity reserves including instruments, amounts, currencies, account information, custody arrangements, etc.

3. Information requirements: Contractual arrangements

3.1. Legal review of the terms and conditions of the contracts governing service provision should be conducted to assess the risks to service interruption. Types of contracts include: contracts for service, software license agreements, SLAs with affiliates, and property and equipment leases. Examples of information requirements to assess the risk to, and to facilitate, the continuity of critical functions could include, but are not limited to:

a) Provider and the contracting entity in the group (distinguish between group-wide contracts and single legal entity contracts);

b) Description of the service;

c) Jurisdiction of service provision and law governing dispute resolution;

d) Contract amount, guarantees, expiry date, termination rights, assignment clauses, change of control provisions, events of default, cure periods, material adverse change clauses;

e) Description of arrangements to allow for services to be extended to acquirer(s) of the failed entity(s);

f) Authorised users under software licenses;

g) Software support arrangements (outsourced vs. internal); and

h) Retention clauses and employment terms for critical staff.

3.2. A method to determine the relative priority of contracts in resolution should be considered. Factors affecting the priority of a contract may include:

a) Delivery of a critical shared service would be jeopardised if the service provider's service were unavailable;

b) Ability and time required to replace the service provider (i.e., substitutability); and

c) Jurisdiction of the service provider.

3.3. A description of the governance framework along with the roles and responsibilities for each division that manages service provision arrangements. Supplier risk management frameworks can be leveraged in resolution to facilitate the continuity of service provision and manage service disruptions should they occur.

Supplementary note (2024)

Digitalisation of critical shared services: Implementing the FSB Guidance on Arrangements to Support Operational Continuity in Resolution

1. Introduction

The FSB Guidance on Arrangements to Support Operational Continuity in Resolution[10] published in 2016 ("Guidance") assists supervisory and resolution authorities and financial institutions to evaluate whether financial institutions that are subject to resolution planning requirements ('firms') have appropriate arrangements to support operational continuity if the firm enters resolution. To resolve a failing firm in a manner that maintains continuity of its critical functions, it is important that there is continuity of critical shared services, such as information technology infrastructure and software-related services, which are necessary to support the continued provision of critical functions.

As part of the digitalisation of the financial services sector, financial institutions have increased their dependencies on third-party service providers in supporting critical shared services in recent years. This can bring multiple benefits to financial institutions including flexibility, innovation and improved operational resilience. However, if not properly managed, disruption to critical shared services could affect the continued provision of critical functions, posing risks to orderly resolution and, in some cases, financial stability.

In that context, the FSB conducted a review in 2023 to assess the application of the Guidance in an evolved context where firms are increasingly relying on third-party service providers. The review found that the Guidance is still appropriate, despite subsequent changes to the technological landscape. The concepts and expectations set out in the Guidance and its principle-based approach are generally applicable to all types of critical shared services. In particular, the Guidance already considers third-party provision of critical shared services. However, the increased use of services that are digital in nature could create specific issues for firms in implementing arrangements to support operational continuity in resolution, such as contractual provisions, mapping of services, governance arrangements, or rights of use and access to operational assets in resolution. In December 2023, the FSB published a report on Enhancing Third-Party Risk Management and Oversight,[11] to address, in some contexts, similar issues in a going concern capacity. This note leverages concepts from that toolkit, where appropriate.

Based on the findings from the FSB's review, this supplementary note to the Guidance provides some clarifications to authorities and firms on the implementation of the Guidance in the context

---

10 FSB (2016), *Guidance on Arrangements to Support Operational Continuity in Resolution*, August.

11 FSB (2023), *Enhancing third-party risk management and oversight: a toolkit or financial institutions and financial authorities*, December.

of the increased dependencies on third-party service providers of critical shared services, and the digitalisation of such services.

2. The concept of operational continuity

2.1. Critical shared services and critical functions

Section 2 of the Guidance describes the concept of operational continuity, critical shared services and critical functions. The Guidance defines a "critical shared service" as "an activity, function or service performed by either an internal unit, a separate legal entity within the group or an external provider, performed for one or more business units or legal entities of the group, the failure of which would lead to the collapse of (or present a serious impediment to the performance of) critical functions". Critical functions are "activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity and cross-border activities".[12]

While this note refers to "critical shared services" in line with the Guidance, it also acknowledges the term "critical service" used in the FSB report on Enhancing Third-Party Risk Management and Oversight and defined as a "service provided to a financial institution whose failure or disruption could significantly impair a financial institution's viability, critical operations, or its ability to meet key legal and regulatory obligations". In practice, some jurisdictions have implemented the Guidance using a wider scope of application that goes beyond critical shared services, to include services that support a firm's viability and the continuity of its critical operations.

Recognising that technology innovations in the financial system are fast evolving, this note does not attempt to define what a digital service is. It acknowledges that critical shared services, whether operational or finance-related, can be digital in nature and that the trend toward digitalisation has increased since the Guidance was published. This evolution can be characterised by the fast migration from services of a more physical nature, including tangible assets, such as equipment and IT hardware, to services of a more digital nature, such as software, data, cloud services, and distributed ledger technology.

2.2. Operational continuity as a going concern supervisory consideration

Section 2 of the Guidance also sets out the interaction between operational continuity in resolution and as a going concern supervisory consideration. Among other aspects, it refers to going concern operational continuity in the context of a firm's resilience and its ability to recover business operations in response to incidents such as IT failures and cyber-attacks. The FSB report on Enhancing Third-Party Risk Management and Oversight sets out a toolkit for the management of third-party risk in going concern. From a resolution perspective, the increased reliance of firms on third-party service providers and the digitalisation of services may mean that, if not properly managed, disruption to critical shared services could precipitate resolution or

12 FSB (2013), *Guidance on Identification of Critical Functions and Critical Shared Services*, July.

disrupt resolution execution in some cases. Firms should have sufficient understanding and oversight of the services provided by third parties to ensure operational continuity in resolution. In line with the Guidance, actions aimed at improving operational continuity in the context of digitalisation of services should consider implications for both going concern and resolution.

3. Service delivery models and resolvability

Section 3 of the Guidance describes, at a high level, the different service delivery models that firms typically adopt for the provision of operational services. The three models set out in paragraph 3.1 of the Guidance – provision of services by (i) a division within a regulated legal entity, (ii) an intra-group service company, and (iii) a third-party service provider – continue to adequately capture the models adopted by firms in the delivery of services. However, with the wider use of third-party service provision and digitalisation of services, authorities and firms should consider whether specific elements could make operational continuity in resolution more complex. For example, with the digitalisation of services:

- Data is increasingly stored and processed across borders. Operational assets may involve assets shared among multiple firms, such as with the use of cloud services, which may lead to uncertainty in ownership and in access to data in a resolution scenario. This leads to a greater need for firms to ensure a full understanding of ownership of and access to these assets in resolution.

- Services can involve more complex and increasingly specialised supply chains, including the use of nth-party service providers[13], as some third-party service providers depend on other IT providers based on sub-contracting arrangements. These trends may add complexity in the service delivery models and, if not adequately captured in the firm's operational continuity arrangements, this could create potential challenges in resolution.

In this context, authorities should also consider how the mixed use of service delivery models, as described in the Guidance, may affect firms' resolvability and operational continuity in resolution.

4. Possible arrangements to support operational continuity

While the Guidance remains appropriate, this note provides some clarifications to the possible arrangements to support operational continuity set out in section 4, specifically for services that are digital in nature.

---

13 According to the FSB report on *Enhancing Third-Party Risk Management and Oversight*, nth-party service providers may be referred to as "sub-contractors, sub-outsourced service providers or indirect service providers". A supply chain refers to "The network of entities that provide infrastructure, physical goods, services and other inputs directly or indirectly utilised for the delivery of a service to a financial institution. For the purposes of the toolkit, the scope of supply chain is limited to the services under a third-party service relationship".

4.1. Contractual provisions

Paragraph 4.4 (i) states that firms *should have clearly and comprehensively documented contractual arrangements and service-level agreements*, with further details provided in paragraphs 4.6 and 4.7.

The increasing use of third-party service providers due to the digitalisation of services, and their supply chains involving nth-party service providers, may make terms and conditions in contracts more difficult to understand, especially as subcontracts may be increasingly technically specialised. Besides, concentration of service provision among a few third-party service providers may make the negotiation of contractual provisions more challenging to continue services in resolution and make it more difficult to easily switch providers due to proprietary technical features or switching costs.

In response to these challenges, firms should have an understanding of contractual arrangements in terms of networks of interdependencies of service providers, both intra-group and outside the group, for the provision of critical shared services that are digital in nature. For instance, firms may consider conditions governing sub-contracting to nth-party service providers. Firms should have the ability to assess potential impediments to operational continuity in resolution that arise from any weaknesses in contractual arrangements.

4.2. Management information systems

Paragraph 4.4 (ii) refers to a *clear taxonomy of shared services and the maintenance of up-to-date mapping of services to entities, businesses and critical functions.*

Digital innovation has introduced new types of services and providers. In their mapping of critical shared services as per the Guidance,[14] firms should consider their third-party service providers' supply chains, to the extent they could affect the continuity of critical shared services in resolution. Consistent with the principle of proportionality and a risk-based approach, firms are expected to identify key nth-party service providers that are knowingly essential to the delivery of critical shared services to support operational continuity in resolution.

4.3. Robust pricing structures

Paragraph 4.4 (iv) states that *cost and pricing structures for services should (…) be predictable, transparent and set on an arm's length basis*.

As mentioned in 3.1, with a high concentration of third-party service providers due to the digitalisation of services, it may be more challenging for firms to negotiate contractual provisions, which may affect the predictability of costs. It is important that firms continue to ensure that cost and pricing structures are predictable before and during the resolution.

[14] The Guidance includes an Annex on indicative information requirements to facilitate operational continuity, including a clear mapping between critical shared service providers and recipients.

4.4. Operational resilience and resourcing

Paragraph 4.4 (v) states that *critical shared services should be operationally resilient* and that they *should not be unduly affected by the failure or resolution of other group entities.*

Firms may choose to increase their use of a given service provider for purposes of efficiency and resilience. At the same time, critical shared services provided by the same service provider may increase the overall impact of a disruption, creating concentration and concentration-related risks.[15] Firms should consider the implications of concentration of providers of critical shared services.

In the event of disruption, substitutability of services may be a viable option to maintain the continuity of critical functions and core business lines during the stabilisation and restructuring phases of resolution. That said, some services are challenging to substitute and developing options to exit over a short term may not always be feasible without undue costs or risks to the financial institution. Firms should pay particular attention to critical shared services that are digital in nature and for which there is a significant risk of disruption due to lack of substitutability.

4.5. Governance

Paragraph 4.4 (vi) states *that critical shared services should have their own governance structure and clearly defined reporting lines.*

The increasing use of third-party service providers for services that are digital in nature may lead to additional complexities for firms to manage proper and effective governance arrangements relating to critical shared services. In this context, firms should pay particular attention to governance arrangements relating to the digitalisation of services.

4.6. Rights of use and access and cross-border provision of shared services

Paragraph 4.4 (vii) states that *access to operational assets by the critical shared service provider, the serviced entities, business units and authorities should not be disrupted by the failure or resolution of any particular group entity.* In addition, paragraph 4.10 notes that *ensuring operational continuity may be more difficult when services are provided by an entity outside of the jurisdiction of the resolution authority (or resolution authorities)*.

The increasing reliance on third-party services and the use of digital technologies[16] may bring more challenges for firms to access their data in a timely manner to support operational continuity in resolution. It also involves greater cross-border provision of services, with data storage and processing potentially located in a different jurisdiction from that of the firm and the resolution authority.

---

15 FSB (2023), *Enhancing third-party risk management and oversight: a toolkit or financial institutions and financial authorities*, December.

16 For example, distributed ledger technologies (DLT) rely on a distributed model of data storage and processing, which may create challenges in terms of ownership or access rights.

Firms should ensure continued access during resolution to intangible assets, such as data processed or stored by a third-party service provider, both locally and offshore. Firms should, to the extent possible, consider in their resolution planning the potential impediments to their rights of access to critical data held by third-party service providers. To the extent possible, they should ensure that their contractual arrangements are resilient and support robust data access to enable appropriate access in resolution to critical firm data stored on a third-party system either domestically or in other jurisdictions.