Client Service Resilience Policy

Version No	4.2
Document Type	Policy
Parent Document	Enterprise Risk Management Framework
Parent Framework	Operational and Technology
Document Approver Name	Ana Chavez alanis
Document Approver Job Title	Global Head of Resilience Risk
Document Owner Name	Christopher John Williams
Document Owner Job Title	Head, OTCR, Resilience Risk,?Policy & Regulations
Document Contact Name	Padmavathy Balasubramaniam
Document Contact Job Title	Senior Manager, OTCR, Resilience Risk
Business Scope	All Businesses
Function Role	All Functions
Geography Scope	GLOBAL
Approval Date	24/03/2023
Effective Date	31/03/2023
Next Review Date	01/10/2025

Table of Contents

Version Control Table

Name	Changes made	Materiality	Approved by	Version number	Approval Date	Effective Date
Padmavathy Balasubramaniam	Migration to Inline format- Non Material Change(No change to document content)	Non-Material	Ana Chavez alanis	4.2	24/03/2023	31/03/2023

The full version history is included in *Appendix.*

1. PURPOSE AND SCOPE

The Client Service Resilience Policy is mapped to the Client Service Resilience Risk Sub-Type within the Operational & Technology Risk Type Framework and sets out the requirements that ensure the Group's services remain operationally resilient.

This Policy details the mandatory requirements across 4 areas of resilience:

- Operational Resilience
- Operational Continuity in Resolution ("OCIR")
- Business Continuity Management ("BCM")
- Crisis Management ("CM").

The Policy supports other Policy Owners in their responsibilities regarding the operational resilience of the Group's services. "Services" are defined as a combination of activities that the business provides which deliver a specific outcome to an identifiable user. The outcome should be distinguishable as a separate service (e.g., Cash Payments) and not as a collection of services (business lines/products).

Services are distinct from "processes" which facilitate the delivery of a service (e.g., payment processing) and can be one of two types:

- External service: A service delivered to an external end user or participant is called a 'Business Service'
- Internal service: Internal services supporting internal operations of the firm (e.g., payroll).

Services should be tiered relative to their materiality for the organisation, its clients and to the markets in which the Group operates. The tiering of services is required to prioritise resources that ensure effective operational resilience, establishing differentiated resilience requirements necessary for the continuity of service and its underlying operational assets. It is recognized that the Group has currently identified services only to the level of Important Business Services ("IBSs"). Further work may be needed to identify other services which are not classified as IBSs.

Specific resilience requirements relating to Technology assets are set out in the Group Technology Policy.

The requirements detailed in this Policy apply to the branches and subsidiaries under Standard Chartered PLC (the Group). Where there is a difference between a local regulatory requirement and Group Policy and Standards, the more stringent of the two shall be complied with.

2. MANDATORY POLICY STATEMENTS

2.1. OPERATIONAL RESILIENCE

Important Business Services ("IBSs") are a relatively short list of external clients facing prioritised services for which the Group has chosen to build high levels of operational resilience through the life cycle of the service in anticipation of operational disruption.

Key requirements include:

i. Identification and approval of IBSs and Impact Tolerance Statements ("ITSs") for each IBS.

ii. Mapping of processes and operational assets (people, technology, facilities, information and third parties) that supports the delivery of an IBS.

iii. Testing of the Group's ability to remain within the ITS for each IBS in severe but plausible disruption scenarios, identification, and remediation of resilience vulnerabilities.

iv. Preparation of self-assessments.

v. Ongoing governance including a monitoring regime and resilience vulnerability management.

2.1.1 Important Business Services

i. Business Segment and/or Product Heads must identify their IBSs annually at a minimum or sooner if a significant change occurs by following an agreed methodology for IBS identification.

ii. Business Segment and/or Product Heads must appoint an IBS owner for each of the IBSs.

iii. Business Segment and/or Product Heads must cascade all IBSs agreed at Group level to Country CEOs and / or COOs of the countries in scope of the IBS.

2.1.2 Impact Tolerance for Important Business Services

i. The Group must be able to articulate its tolerance for impact to an IBS. The IBS Owner must set at least one ITS for each IBS identified. The ITS should specify the maximum tolerable duration of disruption to an IBS beyond which it could pose intolerable harm to clients, stability of financial markets or the Group's safety and soundness. IBS Owners must review ITSs at least annually or sooner if there is a change in the IBS.

ii. Country CEOs and/or COOs of the countries in scope of the IBS must review and acknowledge the ITS set at Group level for each IBS. The Group ITS must be followed as a minimum for all in scope countries unless the country has a more stringent regulatory requirement in which case this should be documented in the Country Addendum.

2.1.3 Mapping

i. IBS Owners must identify the processes/activities and operational assets which support IBS. Through this mapping the impact of a disruption to an operational asset or the weakness in the resilience of an operational asset can be assessed against the ITS.

ii. IBS Owners must review and document the processes/activities supporting IBSs and operational assets such as technology, information, third-parties, facilities, and people that are required to deliver each IBS. The level of details mapped for each IBS should be sufficient to facilitate identification of resilience vulnerabilities and testing of the ability to remain within ITSs for each IBS. Mapping of operational assets supporting each IBS must be updated at least once a year, or sooner if there is any change in the IBS.

iii. The Business must complete a materiality assessment of the operational assets that support IBSs in order to guide the implementation of appropriate resilience capabilities for IBSs to remain within ITSs during severe but plausible disruption.

iv. IBS Owners must engage relevant stakeholders of the countries in scope of the IBSs to complete the mapping of operational assets supporting the IBSs.

2.1.4 Managing Operational Resilience

i. IBS Owners must manage the resilience of IBSs through their life cycle, with emphasis on how IBSs are designed and built with resilience in mind, changed whilst avoiding disruptions, maintained through crises, and wound down.

ii. IBS Owners/Business must define additional resilience requirements for IBSs to remain within ITSs during severe but plausible scenarios including remediation of IBS vulnerabilities within regulatory timelines.

iii. Process Owners for those processes supporting the delivery of IBSs, must capture resilience risks and controls relevant to their remit including risks and controls associated with the underpinning operational assets (i.e., technology, third parties, facilities, people, and information) supporting IBSs as per the Risk and Control Self-Assessment process explained in Group Operational Risk Standard.

iv. For those third parties (including relevant sub-contractors) that materially support one or more IBS, the Contract Owners must ensure third parties can maintain services during disruptions to a level which supports IBSs remaining within ITSs.

v. For those systems and the technology infrastructure mapped to IBSs, Technology Process Owners / Technology Service Owners must ensure recovery times during severe but plausible disruption are aligned with the impact tolerance levels.

2.1.5 Identification of Vulnerabilities to Operational Resilience

i. Process Owners in the Business and Functions supporting IBSs must identify vulnerabilities to operational resilience and instigate controls through Risk and Controls Self-Assessment (RCSA) process as described in the Group Operational Risk Standard to ensure operational assets and the Group's services as an aggregate of those operational assets can be maintained within the resilience requirements defined in Business Impact Assessments (BIAs).

ii. IBS Owners must additionally identify severe but plausible scenarios against which to stress test the operational resilience of IBSs to ensure ITSs can be maintained and / or to identify vulnerabilities to be remediated.

iii. IBS Owners must engage relevant stakeholders of the countries in scope of the IBSs and inform them the vulnerabilities to operational resilience, the mitigation controls and long-term remediation plans in a timely manner. Country CEOs and/or COOs must ensure that remedial actions to resolve vulnerabilities in country are completed in a timely manner with appropriate support.

2.1.6 Remediate Vulnerabilities to Operational Resilience

i. Process Owners in the Business and Functions supporting IBSs must remediate vulnerabilities to operational resilience by following the Response Management Framework as described in the Group Operational & Technology Risk Standard. Remediation of vulnerabilities to IBSs should be prioritized ahead of remediation to other services if a resource choice is required.

2.1.7 Governance

i. Chief Transformation, Technology & Operations Officer (SMF 24) holds responsibility for establishing operational resilience requirements.

ii. Group Head, CCIB and Group Head, CPBB hold responsibility to implement and execute the operational resilience requirements and reporting in their respective areas.

iii. Group Head Resilience is responsible for setting the standards for the identification of IBSs and ITSs and for completing self-assessments, providing the tools for the maintenance of the operational assets mapped to IBSs, defining the standards for scenario testing, and developing a minimum set of metrics to monitor IBSs.

iv. Heads of Business Segments and/or Products must implement processes for all requirements set out as per 2.1.1 to 2.1.6. They must also review IBSs, ITSs and self-assessments in their respective products/ segments annually at a minimum or in the event of material change.

v. The SCB PLC Board must approve IBSs, ITSs and the Group self-assessments on an annual basis.

vi. IBS Owners / Business must:

   a. Ensure IBSs and ITSs are approved by the relevant Business Non-Financial Risk Committee ("NFRC"), other Risk Committees and obtain approval from the Board following the annual validation or in event of any change.

   b. Ensure ITSs for all IBSs approved by the Board are cascaded to relevant stakeholders promptly.

   c. Ensure resilience risks and control weaknesses identified, including during scenario testing, are recorded in the Group Operational Risk system in a timely manner (i.e., as per the timeline stated in the Group Operational & Technology Risk Standard) and are tracked to completion.

d. Monitor all resilience vulnerabilities impacting IBSs and present a resilience dashboard at the relevant Quarterly/Monthly Performance Reviews ("QPR/MPR") and/or Risk Committees.

e. Prepare a written self-assessment for each IBS to evidence the Group's compliance with operational resilience regulation and provide assurance that the Group is able to deliver its IBSs within impact tolerances during severe but plausible scenarios. Self-assessments should include lessons learned during scenario testing and treatment plans to address vulnerabilities. Such self-assessments should be approved by the relevant global business Risk Committee.

vii. Head, Operational Resilience CCIB and Head, Operational Resilience CPBB must:

a. Ensure Consolidated Group self-assessments are reviewed by the relevant risk committees and regularly approved by the Board. This review should also cover the prioritisation of IBSs and investment decisions for the activities required to remain within tolerance level for IBSs during severe but plausible scenarios.

b. Ensure risk management associated with supporting risk types - Third party Risk, Technology Risk, Change Management, Product Management, People Management, Safety and Security and Information and Cyber Security ("ICS") risk are aligned with operational resilience requirements.

viii. Head, Operational Resilience Geographies must monitor local laws and regulations impacting operational resilience and ensure country addendum is developed if the country has more stringent regulatory or business requirements. If there is a need to identify country specific IBSs or ITSs, appropriate agreement must be reached with the IBS Owner at the Group level and the Operational Resilience Head of the business.

ix. Process Owners in the Business and Functions supporting the delivery of IBSs, should incorporate controls to support resilience to the extent that ITSs are attained for each IBS during severe but plausible disruption.

2.2. OPERATIONAL CONTINUITY IN RESOLUTION ("OCIR")

Operational Continuity in Resolution sets the framework to ensure continuity of critical services to facilitate recovery actions, orderly resolution, and post-resolution restructuring. The critical services are those services that need to be available to one or more business units of a firm or entity of a group to provide functions critical to the economy.

OCIR requirements are based on a framework encompassing six pillars:

1. Identification of Critical Economic Functions ("CEFs") and Core Business Lines ("CBLs")
2. Maintenance of the Group operating model via the Service Catalogue
3. Maintenance of OCIR and FMI playbooks
4. Calculation and liquidity management of financial resilience for resolution
5. Financial Market Infrastructures ("FMIs")
6. Contracts resolution readiness.

2.2.1 Governance Framework

In the OCIR governance framework, the Group Chief Transformation, Technology and Operations Officer ("CTTOO") is formally named under the Senior Manager Regime ("SMR") as the individual accountable for the OCIR governance framework. Following the Group's organisation structure, the OCIR governance framework ownership is delegated to the Chief Operations Officer, Transformation, Technology and Operations and to the Global Head, Resilience.

OCIR first line ownership has been formally delegated in writing from the Group CTTOO to the Country CEOs. Country CEOs are also responsible for local compliance to OCIR regulations and are supported by

their Country Management teams, local SMEs and by Group Resilience. Any instances of noncompliance or of risks should be escalated through the relevant Non-Financial Risk Committees ("NFRCs").

The Group CTTOO must ensure the Group is compliant to OCIR regulations and requirements referenced in this Policy.

The Group Resilience must ensure that OCIR controls are performed, and control failures are escalated in the Group Resilience Senior Managers Regime ("SMR") and the Transformation, Technology and Operations ("TTO") NFRC forums for remediation and/or risk acceptance. Group Resilience must periodically review with Group and Regulatory Liaison to manage future regulations impacting OCIR.

Group Resilience defines the requirements for continuity of access to operational assets and engages other functions to implement the Policy requirements e.g., Property Asset Management for property lease agreements, Supply Chain Management ("SCM") and Group Operational Risk (GOR) for third party arrangements, TO for systems and information assets. Group Resilience also works with Group Finance Planning & Analysis ("FP&A") for financial resilience requirements. Any risks or issues are escalated to the SMR, TTO NFRC or the respective risk committees.

2.2.2 PILLAR 1: Identification of Critical Economic Functions ("CEFs") and Core Business Lines ("CBLs")

Identification of CEFs and CBLs is required to ensure that critical services continue to operate during a recovery and resolution scenario. While CEFs identify what activities are critical to the local economy, CBLs help identify what are critical to the Bank.

CEFs are defined as activities performed in country 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. Identification of CEFs helps understand the impact on critical services during recovery, resolution and restructuring planning. The Group has developed a CEF identification capability that facilitates identification of functions performed in-country for third parties that are critical to the economy.

The CEF Assessment framework determines, at a legal entity level, if a Group product is a CEF and needs to be maintained in resolution. The four key questions are:

- Does the home or local prudential regulator mandate the function as critical to the local market?
- Is the Group's provision of the function sufficiently important to the local market based on market share triggers?
- Will disruption of the function have a negative impact on a significant number of third parties?
- Are there any market structures or operational factors that make the timely substitution of functions to an alternate provider difficult?

a. Country CEOs are responsible for identifying if their entities deliver CEFs.

b. Country Business Heads perform CEF identification every two years.

c. The OCIR Function must maintain a central record of all CEF assessment results.

The Prudential Regulation Authority ("PRA") in Supervisory Statement 4/21 defines Core Business Lines ("CBLs") as business lines and associated services which represent material sources of revenue, profit, or franchise value for a firm or for its group. The Group's CBL approach defines products at the Group level by applying a threshold of 5% of the Group's revenue which is aligned with the product assessment for IBS. Additional products may be added which have strategic importance to the Group and remain core to the Group's strategy.

The CBLs will be assessed every two years together with CEFs. The exercise will be driven centrally by Group CCIB and CPBB Resilience team together with Group OCIR.

2.2.3 PILLAR 2: Maintenance of the Group Operating Model via the Service Catalogue

The regulatory expectation under operational continuity is for the firms to articulate how access to operational assets supporting critical services will be maintained at the point of stress or resolution of a firm. The service catalogue codifies the Bank's operating model through capturing and mapping operational assets to the products and processes for resolution and restructuring planning. The operational assets cover teams, systems, third party arrangements and financial market infrastructure (FMI) that support all services.

a. Process Owners must identify and map dependencies to their processes and ensure these dependencies are kept updated.

b. Process Owners must identify deviations to the Standard Operating Model ("SOM"). that supports the Single Point of Entry ("SPE") resolution strategy. The operating model covers provision of services through services provided in-country and by region hub, group hub and dedicated service companies (GBS). Material deviations or exceptions are to be remediated and/or accepted with rationalisation and approved by the Country Non-Financial Risk Committee ("CNFRC"), the Country Risk Committee ("CRC") or the Enterprise Risk Committee ("ERC").

c. Group Resilience must maintain the capability to ensure that interlinkages within the group and mapping of operational assets is available for restructuring and divestment in resolution.

It is the regulatory obligation to maintain an updated Service Catalogue in a timely manner. Process owners are responsible for updating the Service Catalogue for material changes in the process universe and / or related dependencies.

The information in the Service Catalogue is used to support a post-stabilization restructuring of the Group. The dependencies in the Service Catalogue are used to support divestment scenarios and facilitate the creation of Transitional Services Agreements ("TSAs")

2.2.4 PILLAR 3: Maintenance of OCIR and FMI Playbooks

The OCIR and FMI barrier playbooks support key management actions designed for orderly operational continuity at the point of non-viability (PONV), through the 'resolution weekend' and into bail-in periods. The playbooks define a set of activities and execution steps to aid decision making and support critical services to remain operational despite the failure of any Group entities. Group OCIR and FMI playbooks are to be reviewed by the relevant Group business and functions on an annual basis. For the countries,

a. Country CEOs must confirm on an annual basis that their OCIR Country Playbook is fit for purpose.

b. The OCIR Function maintains a central record of all OCIR Country Playbooks.

c. Regional Heads of Operational Resilience must conduct an annual OCIR Playbook scenario exercise for at least one country.

2.2.5 PILLAR 4: Calculation and Liquidity Management of Financial Resilience for Resolution

The Group calculates and deploys the Financial Resilience (liquidity) required to support critical services through resolution. The analysis is carried on an annual basis to establish the adequate level of resources needed to ensure critical services providers continue to provide services in a stress or resolution event.

a. FP&A must calculate Financial Resilience and complete the relevant templates for PRA109 submission.

b. Global Business Chief Financial Officer ("GCFOs") must provide expert critical cost analysis to establish a consistent and transparent Financial Resilience outcome.

c. Treasury Markets must maintain a segregated portfolio of readily realisable assets for the Financial Resilience provision as directed by Group Finance FP&A.

d. Country CFOs are responsible for maintaining the local Financial Resilience provision in cash in the allocated local operating account for payment to local critical service providers during resolution.

2.2.6 PILLAR 5: Financial Market Infrastructures ("FMIs")

A 'FMI' is defined as a multilateral system among participating financial institutions, including the operator of the system, used for the purposes of recording, clearing, or settling payments, securities, derivatives, or other financial transactions.

The objective of managing FMIs is to ensure that the Group takes all reasonable steps to facilitate continued access to clearing, payment, settlement, and custody services in resolution.

The owners of the FMI relationships ("Contract Owners"), must ensure the continued access to FMI service providers that support their business to fulfil the requirements of the five principles:

1. Identifying FMI relationships
2. Identifying FMIs that provide critical FMI services
3. Mapping and assessment of FMI relationships
4. Usage of FMIs and FMI intermediaries
5. Contingency planning.

2.2.7 PILLAR 6: Third Party Contracts Resolution Readiness

Contractual readiness refers to the inclusion of an OCIR clause in the contract between SCB and the third party. It is to ensure the critical service provider, whether contracted with the Group or Country, should not be able to change the arrangements of service provision as a result of the Group entering a period of stress or resolution. It is expected that the contractual arrangements allow for continued use of services in stress and resolution, provided there is no default on payment obligations.

a. Contract Owners must ensure that contracts for third party arrangements, where assessed for OCIR applicability, include the Group's mandatory OCIR requirements via the relevant OCIR clause or other agreed controls that allows continuity of access during resolution.

b. The Global Head of Property Asset Management must ensure that property leases that are deemed necessary in resolution include the Group's mandatory OCIR requirements via the relevant OCIR clause.

2.3. BUSINESS CONTINUITY MANAGEMENT ("BCM")

BCM sets out the mandatory requirements in the preparation of plans to maintain continuity of the Group's operations during business interruptions. The approach is based on the BCM lifecycle:

- Understand the organisation
- Determine strategy and plans
- Maintenance
- Training and Awareness.

2.3.1 Understand the Organisation

a. Risk Framework Owners ("RFOs") and Integrated Risk Framework Owner ("IRFOs") must provide advice to Business / Functions / geographies on scenarios or risk events with the potential to cause significant business disruption and which must be addressed in the Business Continuity Plans ("BCPs").

b. Global Business CEOs and Global Function Heads must create, maintain, and test processes and controls for BCM.

c. Chief Executive Officers ("CEOs") must take overall accountability for managing risk exposure and the supporting remediation activity within the relevant Non-Financial Risk Committee(s)

("NFRCs"), including making decisions to address continuity gaps identified in the Business Impact Analysis ("BIA") or risk assessment.

d. Risk exposures and remediation must align, where relevant, with identified IBS and their associated ITS. Operational Assets mapped to IBS must consider their continuity requirements in severe but plausible scenarios to support IBS meeting its ITS.

e. Department Continuity Coordinators ("DCCs") must stand as a responsible representative for Business Continuity readiness and activation, consulting with the relevant Operational Resilience Manager to complete the Team BIA.

f. Business/Functions must assess the application of Business Continuity controls to third party arrangements, ensuring that third parties meet the external continuity requirements and that the Group's internal continuity capabilities are maintained for the duration of the contract. This role is the responsibility of Contract Owners as defined by the Third-Party Risk Management ("TPRM") Policy.

g. Business/Functions must ensure that Contract Owners conduct assurance activity as part of onboarding and Service Review Meetings where relevant. This role is the responsibility of Contract Owners as defined by the TPRM Policy.

h. For third parties, Business/Functions must assess the application of Business Continuity controls to enable their continued operation in the event of the loss of the IT systems on which they depend.

2.3.2 Determine Strategy and Plans

a. CEOs must take overall accountability for agreeing the scope of their Business Continuity planning, ensuring, where relevant, alignment with the requirements specified by IBS Owners, providing appropriate approval for the BCPs, Operational Continuity Plans ("OCPs") and Third-Party Continuity Plans ("TPCPs") as well as for activating Continuity Plans as required, contacting appropriate staff and escalating issues as appropriate.

b. Business/Function Heads must appoint and provide guidance to a DCC or a nominated lead which are aligned to the requirements of IBS Owners and other service Owners. They must also activate BCPs as required, ensuring the continuity solution(s) within the BIA are adhered to.

c. DCCs must consult with the relevant Operational Resilience Manager to complete the BCP in the appropriate platform.

2.3.3 Maintenance

a. CEOs must take overall accountability for the annual testing and exercising programme for their specific Country/Business/Function to ensure maintenance of BCM capabilities and alignment with IBS Owners' requirements for testing and maintenance.

b. Business/Function Heads must approve pre and post-test reports and the actions arising from BCP tests and exercises, ensuring either the resolution of issues that are identified from BCP tests and exercises, or risk acceptance by the relevant NFRC(s). All test reports related to IBS, or Operational Assets supporting those services, must be reported to the relevant IBS Owners.

c. DCCs must consult the relevant Operational Resilience Manager regarding BCP testing to manage the resolution of issues and actions identified during BCP tests and exercises.

d. For third parties, Business/Functions must conduct assurance activity as part of onboarding and Service Review Meetings where relevant. This role is the responsibility of Contract Owners as defined by the TPRM Policy.

2.3.4 Training and Awareness

a. CEOs must take overall accountability for BCM related training and awareness requirements to ensure maintenance of BCM capabilities.

b. Business / Function Heads must take responsibility for the delivery of training and awareness to all individuals holding Business Continuity roles in their area.

2.4. CRISIS MANAGEMENT

Crisis Management ("CM") sets out the mandatory requirements to develop and apply the capability to deal with crises by identifying potential causes, mitigating them where possible, and responding effectively when they occur. The approach is broken down into 3 stages:

1. Identification
2. Preparation
3. Response / Continuous Improvement.

2.4.1 Identification

a. RFOs and IRFOs must provide advice to Businesses/Functions/Geographies on scenarios or risk events with the potential to cause significant business disruption and which require a Crisis Management Playbook.

b. Global Business CEOs and Global Function Heads must create, maintain, and test processes and controls for CM.

c. Contract Owners must assess and mitigate CM risk associated with material third-party arrangements, ensuring that external third parties meet the minimum CM requirements as stated in the contract for the duration of the services provided.

d. IBS Owners must ensure their responsibility for the management of a crisis affecting their IBS is clearly defined.

2.4.2 Preparation

a. CEOs and Global Business and Function Heads must:

i. Establish Crisis Management Groups ("CrMGs") and approve the crisis structure for their business or function, appointing a Crisis Coordinator as a single point of contact and facilitator for each CrMG.

ii. Ensure in scope IBS Owners are represented on the CrMG, as required relative to the crisis

iii. Ensure that Crisis Management Plans and Playbooks are developed and exercised as required and staff are practised in their roles.

iv. Provide final approval of new / materially changed Crisis Management Plans and Playbooks.

b. Subject Matter Experts ("SMEs") must:

i. Support Business /Functions/Geographies to develop Playbook(s) to address specific threat scenarios related to their area of expertise and provide scenarios for crisis exercises relevant to their area of expertise.

ii. Support the development and delivery of crisis exercises relevant to their area of expertise.

2.4.3 Response / Continuous Improvement

a. RFOs and IFROs must participate in the Post Crisis Review of crisis events and review the outcomes to ensure the adequacy and completeness of lessons identified and actions taken.

b. IBS Owners must participate in the review of crises affecting their IBS to ensure the adequacy of the lessons identified and actions taken.

c. CEOs and Global Business & Function Heads must:

i. Approve the activation of a CrMG and assess the impact of the crisis.

ii. Set the strategy for managing the crisis, including identifying priorities, deciding on the actions, and providing the resources and direction required to implement the strategy.

iii. Communicate with stakeholders to decide when the crisis has been resolved, providing a stand down response as required.

iv. Ensure a Post Crisis Review is conducted and any issues arising are addressed.

d. Subject Matter Experts must:

i. Consult on the impact of crisis events for business operations and on the application of Playbooks relevant to their area of expertise.

ii. Support the Post Crisis Review relevant to their area of expertise.

e. Crisis Coordinators must:

i. Receive notification of disruptive or potentially disruptive events, applying Escalation Criteria to determine which constitute a crisis and require the activation of the relevant CrMG, deciding whether to recommend escalation to a crisis. Crisis Coordinators must advise those reporting the disruption when a crisis is not declared.

ii. Activate CrMG when disruptive events are escalated to Crisis and seek approval of the decision from the CEOs or their nominated delegate.

iii. Facilitate CM meetings and ensure logistics are in place to support them, issuing situation reports to internal stakeholders on behalf of the CrMG.

iv. Report the activation to the CrMG in the next level of the crisis structure and record CM Events on Crisis Events Tracker.

f. Contract Owners must conduct assurance activity as part of onboarding and Service Review Meetings.

2.5. GROUP RESILIENCE ROLES

Group Resilience provide the following roles and responsibilities for the Operational Resilience, OCIR, BCM and CM Processes:

a. Provide subject matter expertise and advice and guidance on all resilience matters.

b. Provide relevant training and awareness to Group Resilience and to Business/Functions/ Geographies.

c. Governance of the CSR Policy, including:

- Collation of management information and reporting
- Assurance of controls activity and reporting
- Monitoring and escalation of risks and issues to the relevant NFRC.

d. Support Group and local compliance with regulatory requirements.

e. Provide globally centralised capability such as platforms, exercises, testing, regulatory reporting.

3. RESPONSIBLE ROLES FOR IMPLEMENTING THE MANDATORY POLICY STATEMENTS

Business and Functions Roles

i. Group COO
ii. Country and Business COOs
iii. Heads of Business Segment and/or Product
iv. Heads of Functions
v. Regional and Country CEOs
vi. Group CFOs
vii. Country CFOs
viii. Global Head, Property Asset Management
ix. Head Group Finance, Financial Planning and Analysis
x. Head Treasury Markets
xi. Global Head, Supply Chain Management
xii. IBS Owners
xiii. Contract Owners
xiv. Outsourcing Owners
xv. FMI Owners
xvi. Business Technology Service Owners
xvii. Department Continuity Coordinators / Nomination Lead
xviii. Crisis Coordinators
xix. OCIR Country Coordinators

Resilience Roles

xx. Group Head, Resilience
xxi. Head, Operational Resilience CCIB
xxii. Head, Operational Resilience CPBB
xxiii. Head, Operational Resilience, Geographies
xxiv. Regional Heads, Operational Resilience
xxv. Cluster/Country Heads, Operational Resilience
xxvi. Head, OCIR Resilience

Risk and Governance Roles

xxvii. Policy Owners
xxviii. Risk Framework Owners
xxix. Process Owners
xxx. Integrated Risk Framework Owners

4. POLICY RELATED AUTHORITIES

The principles in this policy must be fully complied with in full unless a dispensation has been granted. All dispensations must be approved by the Policy Owner and recorded centrally in GovPoint.

5. CONNECTED PROCESSES AND ACTIVITIES

This policy applies to the following Processes:

- Client Service Resilience | Business Continuity Management
- Client Service Resilience | Crisis Management
- Client Service Resilience | Operational Continuity in Resolution
- Client Service Resilience | Operational Resilience
- Technology | IT Service Continuity Management
- For Vendors and Outsourcing arrangements including intragroup outsourcing:
  - Source to Pay | Source to contract
  - Source to Pay | Vendor Management
- For non-Vendor - Other Processes that use Third Party arrangements.

6. POLICY EFFECTIVENESS REVIEW

The Document Owner will monitor effectiveness of this policy through key controls embedded within the processes of Operational Resilience, OCIR, Business Continuity Management and Crisis Management.

7. INTERCONNECTED POLICIES & STANDARDS

Policy Name	Risk & Risk sub-type	Policy Owner	Area of connection
Group Third Party Risk Management Policy	Enterprise Risk Management Framework RTF /Third Party Risk	Global Head of Risk, Functions& Operational Risk	To ensure services provided by third parties and sub outsourcing / fourth parties are aligned with the Bank's Operational Resilience requirements and third-party dependencies are well managed where third parties are involved in any of the processes in delivering IBS, OCIR and BCM to clients. To ensure risk owners identify any specific resilience contingency requirements which the risk owner deems are insufficiently covered by the Group's continuity and crisis management capabilities. To ensure the risk owner articulates any specific requirements pertinent to their risk or operational asset type which would support our services withstand and absorb disruptions rather than rely on continuity and recovery capabilities. This is particularly pertinent for the initial build phase of a new

Policy Name	Risk & Risk sub-type	Policy Owner	Area of connection
			capability/product/service. For example, the articulation of maximum concertation of services against a single operational asset such as a vendor, IT system, building.
Group Technology (IT) Policy	Operational & Technology RTF/ Technology Risk	Global Head of Risk, Functions & Operational Risk	To ensure that technology asset information is accurate and available to support IT service continuity management activities for technology services. To ensure that technology services have defined resilience capabilities that are proven to meet agreed objectives and service levels.
Group Data Conduct Policy	Compliance Risk/Data Management Risk	Global Head of FCC, Conduct & Compliance Framework	Dependency on accurate, reliable, and timely data in support of Bank obligations in the event of crisis or resolution.
Group Health, Safety and Security Policy	Operational & Technology RTF/Safety and Security Risk	Group Head Property	Creating a safe, secure, and healthy environment for staff and clients. Protection of property and physical assets, according to health and safety standards and resilience requirements. To ensure key locations and facilities are protected from external events and that actionable measures are in place in the event that the security, the availability, or the usability of any of those locations and facilities are compromised, in alignment with impact assessment of related IBS. To ensure risk owners identify any specific resilience contingency requirements which the risk owner deems are insufficiently covered by the Group's continuity and crisis management capabilities. To ensure the risk owner articulates any specific requirements pertinent to their risk or operational asset type which would support our services withstand and absorb disruptions rather than rely on continuity and recovery capabilities. This is particularly pertinent for the initial build phase of a new capability/product/service. For example, the articulation of maximum concentration of services against a single operational asset such as a vendor, IT system, building.
Recovery Plan Policy	Capital and Liquidity Risk/ Prudential – Recovery & Resolution	Treasurer	Ensuring the Bank is operationally prepared, within a pre-existing framework, to deploy a series of Management Actions aimed at restoring the financial position in the event of an extreme but plausible liquidity and/or solvency stress.

Policy Name	Risk & Risk sub-type	Policy Owner	Area of connection
Liquidity and Funding Risk Policy	Capital and Liquidity Risk / Liquidity and Funding Risk	Global Head, ERM and Deputy CRO SC Bank	Ensuring the Bank is operationally prepared, within a pre-existing framework, to deploy a series of Management Actions aimed at restoring the financial position in the event of an extreme but plausible liquidity and/or solvency stress.
Group Information and Cyber Security Policy	ICS RTF/ Information and Cyber Security Risk	Group Chief Information Security Officer (CISRO)	Identification of critical information assets and prioritisation of treatment for potential risks to availability. Mechanisms to prevent, detect, respond, and recover from cyber related threats should be aligned to operational resilience requirements. To ensure risk owners identify any specific resilience contingency requirements which the risk owner deems are insufficiently covered by the Group's continuity and crisis management capabilities. To ensure the risk owner articulates any specific requirements pertinent to their risk or operational asset type which would support our services withstand and absorb disruptions rather than rely on continuity and recovery capabilities. This is particularly pertinent for the initial build phase of a new capability/product/service. For example, the articulation of maximum concentration of services against a single operational asset such as a vendor, IT system, building.
Climate Risk Policy	Model RTF/Climate Risk	Global Head, Climate Risk & Net Zero Oversight	Climate Risk is an integrated risk per Group's ERMF, the potential for financial loss and non-financial detriments arising from climate change and society's response to it. There are two primary risk sub-types which drive financial and non-financial risks from climate change, physical and transition risks. Climate risk is specifically identified as one of the Integrated Risks that BCM helps to mitigate.
Group Contracts Policy	Operational & Technology Risk – Legal Enforceability	Head, Risk and Policy Legal	The Group Contracts Policy sets out the mandatory policy statements which must be complied with when entering a contract on behalf of the Group. Staff who execute a contract on behalf of the Group or otherwise commit the Group to a contract, must ensure that the contract is approved by Legal or in a Standard Form approved by Legal. This requirement is linked to the "Third Party Contracts Resolution Readiness" pillar of OCIR & FMI.
Tax Policy	Operational	Global Head,	All Intra-Group transactions must be priced in

Policy Name	Risk & Risk sub-type	Policy Owner	Area of connection
	and Technology	Central Tax	accordance with the internationally recognized arm's length principle as set out in the OECD Transfer Pricing Guidelines. This requirement has been factored into the "Third Party Contracts Resolution Readiness" pillar of OCIR to comply to regulatory obligations.
Digital Assets Risk Management Policy	Enterprise Risk Management Framework RTF / Digital Assets Risk	Global Head ERM & Deputy CRO SC Bank	The policy sets out the requirements for the identification, assessment and management of risks associated with Digital Assets ("DA") exposure or activities arising from the Group's clients, products and projects. As DA related risks are cross-cutting in nature and may materialize through the Principal Risk Types ("PRTs"), existing PRT policies, standards and risk assessments must continue to be complied with.

Standard Name	Risk & Risk sub-type	Standard Owner	Area of connection
People Leader Standard	Operational & Technology RTF/People Management	Group Head, Human Resources	To ensure adequate capability and capacity in the teams that are crucial for the delivery of IBS. Job descriptions must be aligned to the capabilities required to deliver IBS. To ensure risk owners identify any specific resilience contingency requirements which the risk owner deems are insufficiently covered by the Group's continuity and crisis management capabilities. To ensure the risk owner articulates any specific requirements pertinent to their risk or operational asset type which would support our services withstand and absorb disruptions rather than rely on continuity and recovery capabilities. This is particularly pertinent for the initial build phase of a new capability/product/service. For example, the articulation of maximum concentration of services against a single operational asset such as a vendor, IT system, building.
IT Service Continuity Management Standard **IT Resilience Management**	Operational & Technology RTF/Technology Risk	Head, Technology Governance & Assurance	To ensure all IT systems and Infrastructure including cloud that are mapped to the processes in delivering IBSs are aligned with the Group's Operational Resilience requirements. For example, during disruption, system recovery time, individually and

Standard Name	Risk & Risk sub-type	Standard Owner	Area of connection
Standard			jointly, should be aligned with ITS for each IBS.

8. STANDARDS MAPPED TO THIS POLICY

Risk Type	Title	Standard Owner	Standard Approver
O&T RTF – Client Service Resilience	Operational Resilience Standard	Director, Operational Resilience Programme	Global Head, Resilience
O&T RTF – Client Service Resilience	Business Continuity Management Standard	Head, Crisis Management	Global Head, Resilience
O&T RTF – Client Service Resilience	Crisis Management Standard	Head, Crisis Management	Global Head, Resilience
O&T RTF – Client Service Resilience	Operational Continuity in Resolution and Financial Market Infrastructure (FMI) Standard	Head, OCIR Resilience	Global Head, Resilience

9. GLOSSARY

Term	Definition
BCM	Business Continuity Management is the identification of potential impacts which threaten the Bank and the provision of capabilities for an effective response and recovery.
BCP	Business Continuity Plan documents arrangements that guide the bank to respond, recover, resume and restore to a pre-defined acceptable level of operations following a business disruption.
CBL	Core Business Lines are defined as business lines and associated services which represent material sources of revenue, profit or franchise value for a firm or for its group.
CEF	Critical Economic Functions is a product/activity of the firm whose withdrawal or disorderly wind-down could have a material impact on the UK economy or financial system.
CM	Crisis Management - developing and applying the capability to deal with crises by identifying potential causes, mitigating them where possible, responding effectively

Term	Definition
	when they occur and continuously improving crisis response by identifying lessons learned from previous crisis events.
Client	Any individual or entity with which the Group undertakes business or may potentially undertake business, whether as principal or as agent, including counterparty, customer, broker and intermediary; also including the recipients of research material, actual or potential investors and actual or potential issuers that are to be the subject of research material.
Contract Owners	Persons responsible for the arrangement with the third party.
Critical Services	Critical services comprise those services that need to be available to one or more business units of a firm or entity of a group to provide functions critical to the economy or a firm's Core Business Lines.
FMI	Financial Market Infrastructure- is defined as a multilateral system among participating financial institutions, including the operator of the system, used for the purposes of recording, clearing, or settling payments, securities, derivatives, or other financial transactions
IBS	Important Business Service is a service provided by the Bank or a person on behalf of the Bank to a client which, if disrupted, could cause intolerable levels of harm to one or more of the Bank's clients or pose a risk to the safety, soundness, stability or resilience of the financial system or the orderly operation of the financial markets or safety and soundness of the Bank.
IBS Owner	A named individual with end-to-end accountability for the service provided to clients.
ITS	Impact Tolerance Statement ("ITS") is the maximum tolerable level of disruption to an IBS, as measured by a length of time and any other relevant metrics, reflecting the point at which any further disruption to the IBS could cause intolerable harm to any one or more of the Bank's clients or risk to the soundness, stability or resilience of the financial system or the orderly operation of the financial markets or safety and soundness of the Bank.
MPR	Monthly Performance Review
NFRC	Non-Financial Risk Committee
OCIR	Operational Continuity in Resolution
OCP	Operational Continuity Plans provide the Business/Operations teams with the guidance and the premise to develop workaround solutions to recover business services in the event a critical system becomes inaccessible for a prolonged period.
QPR	Quarterly Performance Review
RF	Refinement Forums

Term	Definition
RTF	Risk Type Framework
SC	The OCIR Service Catalogue (“SC”) maps processes in the Process Universe with underpinning operational assets such as systems, vendors, facilities and people.
Severe but Plausible disruption	A severe but plausible scenario is one where the nature, scale or scope of the event goes beyond pre-considered recovery measures and supporting assumptions. Severe refers to a level where the disruption is sufficient to breach expected recovery times. Plausible refers to being conceptually consistent with what is known to have occurred in the past from a variety of information such as previous incidents or near misses, experienced internally or observed externally, horizon risks, such as evolving cyber threat, technological developments and business model changes.
SMF 24	Senior Management Functions 24 as described in the Senior Management Regime (SMR).
Subject Matter Experts	1LOD experts that work in the functions supporting the business with expertise in their specialist area, e.g., Property Heads, Chief Information Officers, Heads of ICS.
TSA	Transitional Services Agreement

10. APPENDIX - Version Control Table

Name	Changes made	Approved by	Version number
Rachel Low	N/A	Gavin Brown	1.0
Nadia Jacob	• Renamed from “BCM Policy” to “CSR Policy”. • Mandatory BCM statements added and aligned to updated BCM Standard. • New mandatory CM statements as aligned to the new CM Standard. • New mandatory OCIR statements as per the updated OCIR process.	Gavin Brown	2.0

Name	Changes made	Approved by	Version number
Chris Williams/ Ramani Venkatachalam	• Included operational resilience aspects • Inclusion of services requirements • Numerous small clarifications	Gavin Brown	3.0
Chris Williams	• Updates to OCIR for PRA SS4/21 • Updates for BCM and Operational Resilience for third parties and regulatory embedment • Inclusion of Operational Continuity Plans	Gavin Brown	4.0
Chris Williams	• Page alignment corrections	Gavin Brown	4.1