Table of Contents

Policy Details	3
Policy Governance	3
What is the policy objective?	3
Who does this policy apply to?	5
Operational Resilience of Important Business Services	7
Business Continuity Management	9
Business Incident Management	9
Operational Continuity in Resolution (OCiR)	10
Where to find out how to meet the requirements?	11
Version Control Details	13
Appendix 1	14
Appendix 2 – Defining RTO, RPO and Impact Tolerance / MTO	15

Policy Details	
Policy name:	Operational Resilience Framework Policy
Date approved:	18 December 2024
Version number:	3.0
Level 1 Risk Category:	Operational Risk & Resilience
Level 2 Risk Category:	Operational Resilience Planning Risk
Aligns to Group Policy and Type:	Business Continuity Policy (Type A) Group Crisis Control and Management Policy (Type A)

Policy Governance	
Executive Policy Owner / Title:	Nicola Bannister, Enterprise Services Director
Policy Owner / Title:	Andrea Phillips, Director, Enterprise Assurance
Policy Manager / Title:	Adam Stage, Head of Operational Resilience
Policy Approval Route:	Executive Policy Owner[1] and Policy Owner
Document Classification:	Internal

What is the policy objective?

Being operationally resilient is the outcome of robust operational risk management. TSB has obligations to manage operational risks, and maintain operational performance, to meet the objectives of its customers, its shareholders and its Partners (staff members).

Since 2018 the UK regulatory authorities have initiated a shift in our thinking in the following ways:

- Focus attention on the services in which operational disruption could have the biggest impact on customers, the UK financial system or on the bank itself
- Assume that failure is inevitable and therefore balance attention on practicing the response to an incident with the steps to prevent incidents in the first place.

These themes apply to all the components within the Operational Resilience Framework category, namely:

1. Operational Resilience of the Important Business Services (IBS),
2. Business Continuity Management,
3. Business Incident Management; and
4. Operational Continuity in Resolution (OCiR).

The FCA's New Consumer Duty is consistent with the operational resilience regulation insofar as it requires us to look through the lens of the customer, avoid foreseeable customer harm and support customers in pursuing their financial objectives. The operational resilience regulation rightly focuses on the services where operational disruption has the potential to cause intolerable harm to customers. The Operational Resilience Framework

[1] *Note, only material changes to the policy will be sent to Executive Policy Owner for approval. All other changes will be approved by the Policy Owner.*

policy, and supporting standards, helps the bank to assess and improve the resilience of its services to withstand operational disruption, and explains how we are set up to respond when things go wrong.

The Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), together the regulators, have definitions for what constitutes “important business services” for operational resilience and “critical services” for OCiR. The relative importance of activities under Business Continuity Management and Business Incident Management are set by TSB.

The risks being addressed by the policy relate to:

1. Disruption to core business activities leading to impact to services for customers, potential customer harm and financial loss;
2. Inability to operate critical economic functions (CEF) or core business lines (CBL) effectively in a resolution scenario; and
3. Inability to remain within impact tolerances in the event of a severe-but-plausible scenario leading to intolerable customer harm, a risk to the safety and soundness of TSB and increased regulatory scrutiny.

Managing these risks appropriately will provide TSB with comfort that;

- We know which services (or activities) can have the biggest impact on TSB, or the point at which disruption becomes intolerable;
- We understand how they are delivered, and therefore the impact on a service when component parts are disrupted (e.g. an IT application or third party supplier);
- We test our ability to respond and recover to severe but plausible scenarios, which builds confidence in being able to *weather the storm;* and
- We are able to evidence our approach to give confidence to TSB Board members, regulators, shareholders and our customers that we can continue to deliver what is important / critical to them

The underlying Technical Standards are located on the Policy Portal and set out the regulatory requirements, where they exist, for TSB to adhere to as well as expectations set internally by the Policy Owner.

TSB relies upon third parties to deliver its services. We use the bankwide Policy Due Diligence framework run by Sourcing and Supplier Management to review suppliers’ continuity arrangements against the relevant standards within this policy framework.

The table below sets out the common elements for the four different components of the Operational Resilience Framework covering important business services, OCiR, BCM and business incident management. The respective technical standards for each of these components set out further explanation and our expectations.

	Operational Resilience of important business services	Operational Continuity in Resolution[2] (OCIR)	Business Continuity Management (BCM)	
Prioritise "activities"	✔ Important Business Services	✔ OCiR Critical Services	✔ Activities with an MTO <24 or 24-48 Hours.	
Set tolerance for disruption	✔ Impact tolerance	-	✔ Maximum Tolerable Outage	
Map and understand the dependencies	✔	✔	✔	
Set out response and recovery plans	✔ Playbooks by scenario[3]	✔ OCiR Playbook	✔ Business Continuity Plans	Applies to live **Business incident management**
Test ability to respond	✔	✔	✔	
Formal approval	✔ Annual Board self-assessment	✔ Minimum Band G sign-off and 2-yearly TSB self-assessment[4]	✔ Band G sign-off or Band F where direct report to Director	

Note on scenario testing

As the table above clearly shows there is a significant overlap of activities across the different capabilities within this policy. Of particular importance is the act of scenario testing. A single scenario test or exercise can meet multiple requirements if the objectives are set out accordingly and the documented report captures them. For instance, an exercise of our Gold and Silver team as part of Business incident management could be used to draw conclusions on the resilience of our important business services, if the impact is assessed, and also provides an opportunity to test the business continuity plans of impacted areas.

Who does this policy apply to?

All partners who have a role to play in the planning for operational disruption and / or the response and recovery for an operational incident. This includes:

- Important Business Service Accountable Executives and their representatives
- Level 2 Risk category owners within L1 Operational Risk and Resilience
- Business Unit Controllers with Business Continuity responsibilities and their representatives

[2] OCiR is one of 8 barriers to resolution and should be considered within the overall Resolvability Assessment Framework
[3] *Not yet created*
[4] Self-assessment is not currently a requirement but will be expected as part of future TSB resolvability assessments coordinated by Treasury

- Operational Resilience team within Enterprise Assurance
- Major Incident Management team within CIO Cloud & Service Delivery and Business Unit Incident Champions
- CIO colleagues responsible for the design of our infrastructure and services upon which Business Units rely
- Those leading change initiatives (such as Value Stream Leads, Product Owners and Technical Leads) which may impact on the ongoing resilience, or temporary disruption to, the most important services we operate
- Sourcing and Supplier Management colleagues responsible for the supplier management framework
- TSB Supplier Accountable Executives and Supplier Relationship Managers
- Those colleagues with responsibility for TSB's preparedness for OCiR, including those who attest to our OCiR arrangements (e.g. Finance, Treasury, HR, Procurement and CIO).
- Third parties (including outsourcers) responsible for arrangements which contribute to TSB's delivery of important or critical services[5].

Waivers

Waivers to this Policy will be considered. For the definitions, forms to raise requests and guidance refer to the Policy Portal.

Breaches

For any events identified please follow the Event process and guidance detailed in the Event Manual. For further guidance and support please refer to the Events and Breaches SharePoint site and / or Enterprise Assurance.

[5] In reviewing what is acceptable from a resilience perspective for our supply chain we take into account our standards on important business services, business continuity and incident management. These standards support our approach to policy due diligence. We do not take into account our OCiR standard which is more focused on how TSB sets up arrangements with suppliers to be resolution-resilient through contractual arrangements.

Operational Resilience of Important Business Services

What must we do?	How do we check we are doing that? *(ie Monitoring of the control activity)*
IBS Accountable Executives are accountable to TSB's senior management and the Board for the overall resilience assessment of the IBS and leading TSB's approach to meeting the UK regulations. Activity is supported by Level 2 Risk Specialists, with oversight and additional guidance from the EA Operational Resilience Team. The key UK regulations require TSB to: • Identify which services we deliver to our "clients" (as defined by FCA) or "another person" (as defined by PRA) which meet the regulatory definition of important business services (IBS). *(SYSC 15A.2.1, PRA Rulebook 2.1, SS1/21 – 2.2.2.2)*; • Set impact tolerances for each IBS with respect to both the FCA and PRA definitions, though they may be set at the same point. *(SYSC 15A.2.5, PRA Rulebook 2.2, SS1/21 – 3.1, 3.4, 3.5, 3.14, 4.8, 4.10)*; • Map the dependencies required to deliver the IBS. *(SYSC15A.4.1, 15A.4.2, PRA Rulebook 4.1, SS1/21 5.1-5.4, 5.8)*; • Run scenarios to test how we would respond to operational disruption affecting one or more IBS, and whether we could stay within the impact tolerances, *(SYSC 15A.5.1, 15A.5.3, SS1/21 6.1, 6.4)*; • Important Business Service Accountable Executives and L2 Risk Category Owners, with support and oversight from the Operational Resilience Team are responsible for the identification, documentation, tracking and management of exposures which may prevent us from operating within impact tolerances in all severe but plausible scenarios. *(SYSC 15A.4.1, SS1/21 5.3, 5.4)* The TSB Banking Group plc Board ('Board') must regularly review the firm's implementation of the operational resilience framework for the important business services and approve a self-assessment at least once every 12 months. *(SYSC15A. 6.1, PRA Rulebook 6.1-6.3, SS1/21 6.3, 81-8.3)* Representatives of the IBS "pillar" dependencies (most notably Level 2 Risk Specialists for technology, cyber, data governance and data quality and supplier risk) must document and maintain for their pillar details of any dependencies enabling the delivery of an IBS. They must submit resilience data aligned to IBS dependencies on a monthly basis to inform the resilience assessments. More detailed information is captured in the Technical Standard on the roles and	The risk to TSB is that we are unable to meet Operational Resilience regulatory requirements outlined in FCA SYSC 15A. PRA SS1/21 and the PRA Rulebook, leading to a failure of Important Business Services to remain within the defined impact tolerances in the event of a severe but plausible disruption. This could be caused by; • The inability to appropriately identify Important Business Services (IBS), set effective Impact Tolerances and map dependencies for the delivery of those IBS. • The inability to implement effective resilience measures to enable TSB to recover IBS within impact tolerances in the event of a severe but plausible disruption to People, Process, Facilities, Technology, Data and/or Suppliers. This may lead to; • intolerable levels of harm to any one or more customers; • pose a risk to TSB's safety and soundness; or • pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets. We check this by completing the following activity at least annually, and following any material change to the business or the market in which TSB operates; • We follow a principles-based approach to assess which of our activities meet the definition of **'Important Business Service.'** This is approved by a TSB Accountable Executive & by the TSB Board. • Each **'Impact Tolerance'** is in line with TSB's current methodology, recorded as a time-based measure as a minimum (e.g. hours, days or point in time) and using supplementary metrics (e.g. number of transactions) to better understand impact. These tolerances are set by the TSB Accountable Executive for each IBS, reviewed & approved by TSB Board. • Documented dependency **'Mapping'** for each Important Business Service detailing dependencies on: people and business activity, technology, data, third party and property. Mapping is the responsibility of IBS Accountable Executives, but requires support from Level 2 Risk Specialists who own most of the data and with guidance and oversight from Operational Resilience. This should leverage existing tools and knowledge where appropriate (i.e. ServiceNow), and dependencies should be added to

expectations of IBS Accountable Executives and Pillar Representatives. During an operational incident we must be able to identify whether one or more important business services are affected and whether we will breach, or have breached, our impact tolerances for those IBS. This information is reportable to our supervision teams at the PRA and FCA. TSB Partners must ensure that they consider the operational resilience of TSB's agreed important business services when making operational decisions. This consideration is embedded into the processes across the bank including the way that we manage change initiatives and the applications in scope of IT testing.	an appropriate information repository to form a golden source of dependency information for each L2 Risk Category. • Conduct **'Scenario Exercises'** against each Important Business Service validating the ability to remain within Impact Tolerances, based upon areas that underpin delivery (i.e. data, people, suppliers and technology[6]).This activity is facilitated by the Operational Resilience Team with support from IBS representatives and Level 2 Risk Specialists. Where possible, this should leverage existing testing regimes, undertaken & approved no later than 12 months from date last assessed. • Identification and documentation of '**Exposures'** to be remediated, to ensure Important Business Services can be recovered within Impact Tolerances. Exposures may be identified through, Dependency Mapping, Testing (including severe but plausible Scenario Tests), Live incidents and Risk Management activity (including Audits and 2nd Line Risk Reviews). Once an exposure is identified, it should be raised on ARM to ensure it can be tracked and appropriately managed. This is the responsibility of IBS Accountable Executives, but requires support from Level 2 Risk Specialists and guidance and oversight from Operational Resilience. **NOTE:** Some exposures may not be cost effective to remediate completely and will need to be formally risk accepted. • A written **'Self-Assessment'** approved by TSB Board to demonstrate compliance with requirements set out by the FCA & PRA (e.g. FCA SYSC 15A.6.1) no later than 12 months from the date last approved. This is the responsibility of IBS Accountable Executives, supported by the Operational Resilience Team and requires input from Level 2 Risk Specialists.

[6] Note, property is not a key dependency for TSB as we have no offices which are considered to be critical to the delivery of an IBS

Business Continuity Management	
What must we do?	**How do we check we are doing that?** *(ie Monitoring of the control activity)*
TSB must ensure it has a Business Continuity Management (BCM) Framework aligned to business priorities. This includes plans defining the delivery of services to an appropriate level defined by Business Units in the event of disruption, including any workarounds and substitution. This should also address the requirements set out in the Business Continuity Technical Standard. Each business unit must manage its risks and issues within appetite achieving the MTO defined within your BIRA and comply with the standards as defined in the BCM and Incident Management technical standards. Exco members are accountable for appointing a designated Business Unit Controller (BUC) in each Business. The BUC must be a direct report of a Director (Grade H+) and a minimum of Grade F. BUCs are responsible for appointing appropriate people into the roles as defined in the BCM and Incident Management Procedures. Change Management – Business Units must ensure that any project or programme they are sponsoring is assessed to determine the impact on BCM arrangements with due requirements brought into scope of the project/programme	The risk to TSB is interruption to core business activities leading to disruption to services for customers, potential customer harm and financial loss. How we check: • **Business Impact Risk Assessment (BIRA)** is documented in a centrally held template for all Business Areas and is reviewed and approved at least every six months, or following any material change to a Business Unit. • **Business Continuity Plans (BCPs)** are in place and reviewed at least annually and are kept up to date following any significant change to recovery and response processes. • **Business Continuity and Incident Management Testing and Exercising**. The schedule of Tests & Exercises is completed and reviewed at least annually to ensure they are on track and proving required response and recovery timescales. Business units may be able to use a single scenario exercise to support their requirements across multiple standards in the Operational Resilience Framework policy, as long as the appropriate post test report captures the objectives and results appropriately.

Business Incident Management	
What must we do?	**How do we check we are doing that?** *(ie Monitoring of the control activity)*
TSB must ensure it has an incident management framework that leads and directs the initial response through recovery and return to BAU and which complies with the standards as defined in the Business Incident Management Technical Standard. TSB must ensure we have adequate capacity and capability in the key roles of incident secretariat, Bronze chair and Silver chair, along with key	The risk to TSB is interruption to core business activities leading to disruption to services for customers, potential customer harm and financial loss. How we check: • **Business Incident Management Framework** is implemented, embedded and maintained. Documentation is accessible to those in TSB who require it. There are established procedures including, for instance; □ invocation criteria to go to a metal triage call which could lead to a Bronze or Silver incident denomination, □ rotas to ensure skilled chairs and secretariats are available on a 24/7/365 basis,

business representatives to coordinate the incident response in a robust and consistent manner.	▯ processes to ensure appropriate representation at Bronze/Silver calls, ▯ processes for the approval of communications both internally and externally, such as those to regulators; and ▯ templates for consistent communications to ExCo members. • **Recovery plans** are in place (see above on Business Continuity Management). These include **Playbooks** which consider impact on important business services[7] and provide additional information on plans to limit customer harm resulting from an incident, customer treatment strategy and any other relevant information that can help in the resolution of the incident. These are reviewed at least annually and following any identified changes, for example learnings from actual incidents. Periodic training and awareness sessions are run for the benefit of secretariat and chairs to update them on changes to the process and on lessons learned from recent incidents. During an incident it is important to ensure alignment of ExCo communications between CIO Major Incident Management (MIM) and the Bronze chair. This is done through MIM representation on the calls and inclusion of the Head of IT Service Management on the Bronze email updates.

Operational Continuity in Resolution (OCiR)	
What must we do?	**How do we check we are doing that?** *(ie Monitoring of the control activity)*
• Identify all relevant services (i.e. critical), as well as underlying relevant operational assets and staff/roles. (SS4/21 2.6-2.8, 4.2) • Document clear and comprehensive contractual arrangements for both external third-party and intra-group legal entity providers. (SS4/21 6.1) • Assess the operational continuity risks in resolution, such as the interruption of relevant services, loss of access to relevant operational assets and unavailability/vacancy of relevant staff/ roles (e.g. via scenario testing). (SS4/21 11.2-11.3) • Mitigate the identified operational continuity risks by putting in place appropriate operational arrangements to ensure continuity of services during changes to service provision (e.g. resolution-resilient service contracts); (Prevention of preferential treatment) (Objective service level agreements) (Access to operational assets). (SS4/21 11.5) • Have in place predictable, transparent and arm's length cost and pricing structures for services. (SS4/21 8) • Ensure the financial resilience of service providers, through performing due diligence of external third parties and holding sufficient liquid resources for intra-group service providers. This	The risk is that TSB may be unable to meet the minimum three resolvability outcomes: 1. Have adequate financial resources in the context of resolution; 2. Be able to continue to do business through resolution and restructuring; and 3. Be able to coordinate and communicate effectively within the firm and with the authorities and markets so that resolution and subsequent restructuring are orderly. How we check: • Maintenance of a critical service catalogue including people and asset dependencies to deliver each critical service

[7] Historically TSB has required playbooks for "Operational" areas but their usage has been variable. Having playbooks for IBS will ensure robust plans are in place where TSB has the potential to cause the most harm during operational disruption.

is expected to be at a minimum, liquidity resources equivalent to 1/6th of annual fixed overheads of the critical services they provide to the firm (SS4/21 11.6) • Ensure adequate governance arrangements for OCIR purposes (resolution planning and execution). (SS4/21 12.1) • Evidence the above – demonstrate how its operational arrangements facilitate recovery and resolution. (SS4/21 12.2)	• Submissions of service catalogue entries on a half-yearly basis; • Procurement and Legal review of contractual terms in line with contract renewal scheduled; • Scenario testing of the OCiR Playbook; • Calculations for the OCiR liquidity buffer; • Documented arrangements for how the buffer is held in high quality liquid assets; • Documented arrangements for the additional buffer held by Sabadell Digital, as a critical intra-group provider, in case of failure of Sabadell Group; • Management and Governance arrangements are documented for intra-group and intra-entity arrangements; and • Annual attestation of OCiR compliance by control owners.

Where to find out how to meet the requirements?

Technical Standards (see Policy Portal)

- Operational Resilience of Important Business Services
- Business Continuity
- Business Incident Management
- Operational Continuity in Resolution

Procedures / Guidance Documents (see Policy Portal)

- Procedures - Business Continuity
- Methodology - Important Business Services (IBS)
- Methodology - Impact Tolerance
- Methodology – Mapping
- Methodology – Scenario Testing
- First touch audit trail - Self Assessment annual sign off by TSB Board (held on IBS SharePoint site)
- OCiR Playbook

RACI

- Responsibilities under this Policy (Appendix 1 below)

Glossary

Term:	Definition:
All definitions of terms used in the Policy should be included in the Glossary	

Business Continuity	The capability of a business to continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident.
Business Unit Controller (BUC)	Business Unit Controllers (BUCs) have overall responsibility for the governance of all aspects of BCM within their Business Unit.
Impact Tolerance	The maximum tolerable level of disruption to an important business service, as measured by a length of time and other relevant metrics, reflecting the point at which any further disruption to the important business service could pose intolerable harm to any one or more of the firm's clients or intolerable risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the Financial Markets, Act.
Important Business Service	A service provided to one or more clients of the firm which, if disrupted, could: (a) cause '*intolerable levels of harm'* to any one or more of the firm's clients; or (b) pose a risk to the firm's safety and soundness – the impact on the firm itself, including the: o impact on the firm's profit and loss; o potential to cause reputational damage; and o the potential to cause legal or regulatory censure.
Incident Management	Incident management is the process of limiting potential disruption caused by an event, followed by a return to business as usual. Without effective incident management, an incident can disrupt business operations, information security, IT systems, employees, customers, or other vital business functions.
Intolerable Harm	For the purposes of this policy, the point where it would be difficult to put customers back to their correct financial position or where non-financial impacts have been caused to customers due a service disruption that are unable to easily be remediated *(i.e.. mortgage chain collapsing)*
Operational Continuity in Resolution	OCIR[3] is a key component of the UK's Recovery and Resolution Planning (RRP) regime, focusing on the operational arrangements required to ensure the ongoing delivery of critical functions in recovery and resolution.
Operational Resilience	Operational resilience refers to the ability of firms, FMIs and the system as a whole to prevent, adapt and respond to, recover and learn from, operational disruption.
OCIR Critical Services	Activities, functions or services performed for one of more business units of the firm or for the firm and another member of its group, the failure of which could lead to the collapse of or present serious impediment to the performance of the firms critical functions or core business lines.

Key regulation	
Important business service resilience	• FCA Handbook, SYSC requirements (see additional commentary in FCA PS21/3) • PRA Rulebook Operational Resilience part (see additional commentary in PRA SS1/21, PRA PS6/21 and Statement of Policy) In addition, there is a library of industry good practice that is maintained by the Cross Market Operational Resilience Group (CMORG), accessible via their website
Operational Continuity in Resolution	PRA Rulebook Operational Continuity Part
Business Continuity Management	FCA Handbook, SYSC requirements PRA Rulebook: Operational Risk Part and General Organisational Requirements

Business Incident Management	Expectations are part of SUP 15 notifications

Policy Review

This Policy shall be reviewed on an annual basis or following any material change to Regulatory/Policy requirements or to the risks and controls covered by the Policy.

Version Control Details				
Version Number:	**Author:**	**Approval Date:**	**Effective Date:**	**Comments:**
1.0	Adam Stage	20 September 2022	30 September 2022	Draft policy created
1.1	Adam Stage	20 July 2023	20 July 2023	Updated for OCiR changes plus Consumer Duty commentary
2.0	Adam Stage	22 November 2023	1 December 2023	Removal of Director Attestation Certificate for BCM; clarification of policy scope for supplier and change of frequency for OCiR attestation to six-monthly. Clarification that single scenario test may be used to meet multiple standard requirements. Addition of regulation table
3.0	Chris Willoughby	18 December 2024	18 December 2024	Updates to risks, clarification of relevant requirements and documents and to produce a more prescribed responsibility for Important Business Services Accountable Executives.

Appendix 1

- RACI – Policy Management

Exec Policy Owner – Nicola Bannister

Policy Owner / L2RCO – Andrea Phillips

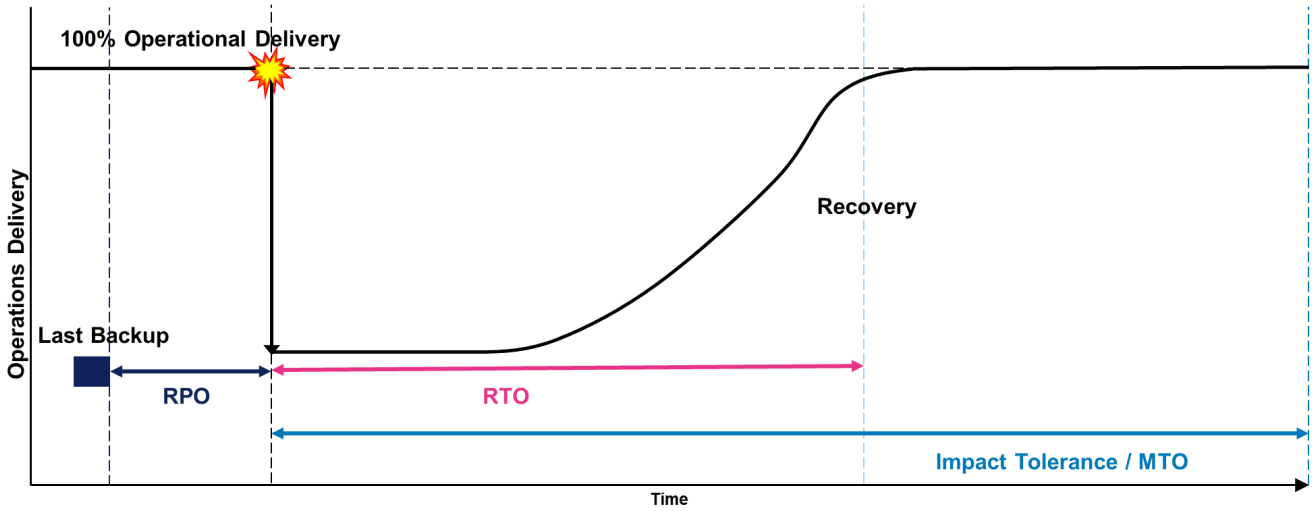
Policy Framework RACI Matrix of Responsibilities

Summary of key policy-related responsibilities. For additional detail please refer to the TSB Policy Framework Manual.

Policy Requirements	KEY		1LOD					2LOD	
			Executive Policy Owner	Policy Owner	L2 RCO	Other Business Units	Enterprise Assurance	RMF Team	Oversight
	Responsible	R							
	Accountable	A							
	Consult	C							
	Inform	I							
Policy Design									
Policy fit-for-purpose: correct template, content accurate, relevant and up-to-date			A	R	C	-	I	C	C
Associated risks are clearly articulated in the policy and policy aligned to Risk Categorisation Model.			A	R	C	-	C	I	C
Control activities within policy are accurate, clearly reflected and fit-for-purpose to mitigate associated risks.			A	R	C	-	C	I	C
Policy updated to reflect any pertinent changes to operating environment (internal and external)			A	R	C	I	C	I	C
Ongoing oversight and challenge on policy design – Alignment to Policy Framework requirements.			I	C	C	-	I	R&A	I
Ongoing oversight and challenge on policy design – Risk and Controls and relevance (alignment to regulation etc).			I	C	C	-	I	C	R&A
Policy Management									
Policy communicated to key stakeholders including Oversight, and where appropriate Procurement and Sabadell.			A	R	I	I	I	I	C
Develop, monitor and refresh any training material required to support policy engagement / awareness (e.g. core learning)			A	R	I	I	I	I	I
Ongoing compliance with relevant policies			-	-	-	R&A	-	-	-
Policy Review and Approval									
Complete annual policy review/Policy Review Statement (PRS) in-line with Annual Review Schedule/Policy Framework requirements.			A	R	C	-	I	I	C
Syndicate annual policy review and PES with key stakeholders, including Oversight and where appropriate Sabadell.			A	R	C	-/C	I	I	C
Policy approved by appropriate governance channel.			A	R	I	-	I	I	I
Updated approved policy and PES provided to RMF team to update Policy Portal			A	R	I	-	I	I	I
Oversight of Annual Policy Review			I	C	I	-	I	R	R&A
Policy Waivers and Breaches									
Request policy waiver where compliance with specific requirements cannot be achieved			I	C	I	R&A	I	I	I
Review and approve/decline policy waiver requests (new waivers and extensions)			C&I	R&A	I	C	I	I	I
Approve/decline policy waiver requests where own business unit unable to comply with policy requirements			R&A	C	I	-	I	I	I
Identify and record policy breaches in-line with Incident process			I	C	I	R&A	C&I	-	I
Request extension to existing waiver where compliance cannot be achieved within agreed timeframe.			I	C	I	R&A	C&I	C&I	I
Check waivers remain valid and up-to-date, challenging non-compliance where appropriate.			A	R	C&I	C/I	C&I	I	I
Monitor ongoing compliance through waiver/breach reporting, challenging non-compliance and identifying requirement to update policy where appropriate.			A	R	C	C	C&I	I	I
Ongoing oversight and challenge (close and continuous / in scope of agreed thematic assurance reviews)			I	C	I	I	I	C	R&A
Policy Framework									
Maintain Policy Framework – Policy Handbook, Policy Portal (SharePoint), templates etc.			I	C&I	I	I	C&I	R&A	C&I
Publish new / updated Policies and technical standards on the Policy Portal.			-	C	-	-	-	R&A	I
Maintain annual review schedule and challenge non-compliance with associated requirements.			C&I	C	I	I	I	R&A	I
Communicate changes to the Policy Framework to key stakeholders including Policy Owners and Oversight.			I	C	I	I	I	R&A	C
Maintain the Central Policy Waiver Log			I	I	I	I	I	R&A	I
Produce and communicate consolidated, accurate Policy-related management information			I	I	I	I	I	R&A	I
Engage Sabadell re Group policy framework – alignment, new policies etc.			I	I	I	-	I	R&A	I

Appendix 2 – Defining RTO, RPO and Impact Tolerance / MTO

The diagram below brings to life some of the key terms and how they relate to the timescale of an incident.



RPO (Recovery Point Objective)

The maximum tolerable data loss following a disruption.

RTO (Recovery Time Objective)

This is the targeted recovery time when a critical activity or process is disrupted. This typically comes at the point in time beyond which there is significant disruption to services and is effectively the risk appetite for disruption.

Impact Tolerance / MTO (Maximum Tolerable Outage)

This is the maximum tolerable disruption before either, 1) Intolerable harm is caused to the end customer (i.e. harm TSB can not put right), or 2) The viability of TSB is threatened.