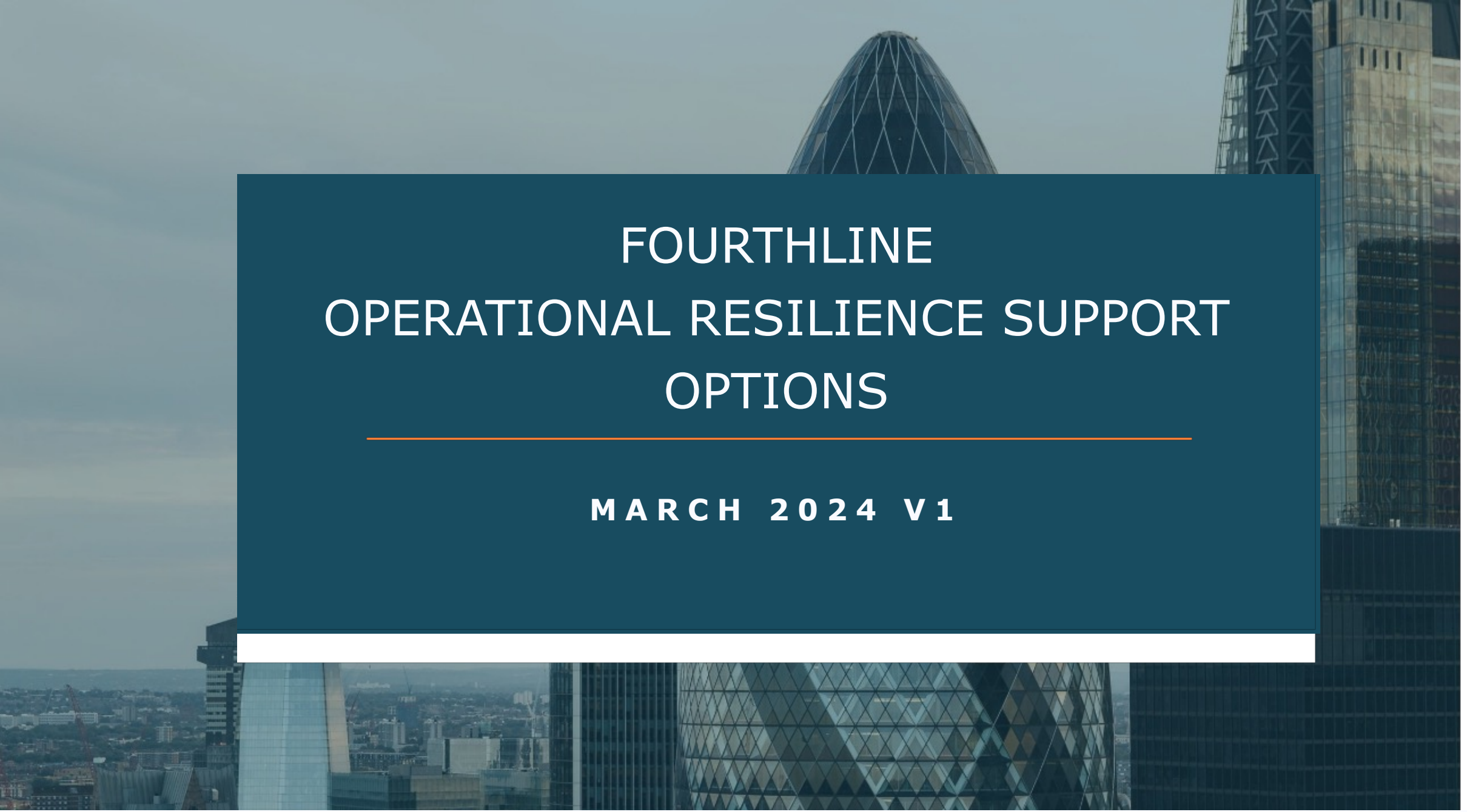


FOURTHLINE OPERATIONAL RESILIENCE SUPPORT OPTIONS

MARCH 2024 V1

FOURTHLINE

Operational Resilience overview

FOURTHLINE

GLOBAL OUTAGES AND REGULATORY OUTLOOK

FCA and PRA

The FCA and PRA issued separate but overlapping operational resilience regulations in March 2021 with a 12 month implementation window and a 3 year transitional period to March 2025 to remain inside impact tolerances.

Hong Kong Monetary Authority (HKMA)

It sets out the HKMA's expectation that every Authorized Institution (AI) should be operationally resilient, and provides highlevel guidance on how AIs can develop an integrated and holistic operational resilience framework to support this.

Monetary Authority of Singapore (MAS)

In June 2022 MAS communicated that all financial institutions will soon be required to specify a recovery time should critical services suffer an outage, including intermittent ones.

Central Bank of Ireland (CBI)

The CBI issued cross-industry guidance on Operational Resilience late in 2021, with a go-live requirement for the OR framework in late 2023.

Australian Securities and Investments Commission (ASIC) Regulation

ASIC Wants Trading Players to Provide Services Even during Outages, asking market players to build resilient measures for outages. It is concerned about the upcoming technology upgrades that might impact operations.

MIZUHO

Mizuho Bank experienced a system failure that disrupted ATMs from around 9 a.m. until around 4:30 p.m. The megabank saw transactions temporarily suspended at about 80% of its ATMs.

aws

AWS experienced extended outages three times within a matter of weeks, affecting services and vendors ranging from Zoom and Quickbooks Online to Xbox Live and Hulu.

TSB

In 2018, 2 million TSB customers were left without access to their current accounts following migration to new data centres. An inquiry identified failure to test as the root cause. 80,000 customers left the bank, which cost the provider £400m.

Basel Committee on Banking Supervision (BCBS)

"Operational resilience is an outcome that benefits from the effective management of operational risk. Activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and the monitoring of risks and control effectiveness work together to minimise operational disruptions and their effects."
- Principles for Operational Resilience Mar 2021

TSYS

In 2021, a problem at 3rd-Party payments firm, TSYS, impacted customers of Natwest, Santander, TSB, Tesco Bank, Halifax, HSBC, Co-operative Bank and Barclays. Customers were unable to access any credit card services, including making a payment.

CommonwealthBank

Due to an outage, Hundreds of customers were left without access to their money. An error message began cropping up for people trying to use the Netbank App and Website, while others claimed they couldn't use their bank cards too.

BENEFITS OF STRONG OPERATIONAL RESILIENCE

FourthLine provide an integrated Risk Management, Technology, Data, Third-Party and Cyber resilience approach. We unlock capabilities to identify, protect against, tolerate, respond and recover from disruptive events, ensuring that firms:

I. **Protect** your important services via proactive risk identification, prevention and detection capabilities

II. Maintain a **readiness to respond** through effective response and recovery capabilities.

OUR ROADMAP FOR ESTABLISHING AND EMBEDDING RESILIENCE

Run & Optimise Resilience

Resilience as a Managed Service:

- **Run - Execution of annual cycle of resilience activities** including critical services, mapping and testing refresh, controls monitoring, testing, assurance and resilience plan maintenance.
- **Optimise – resilience processes & procedures** through **innovative technology solutions** to enable 'identify, prevent, detect, respond and recovery' capabilities.

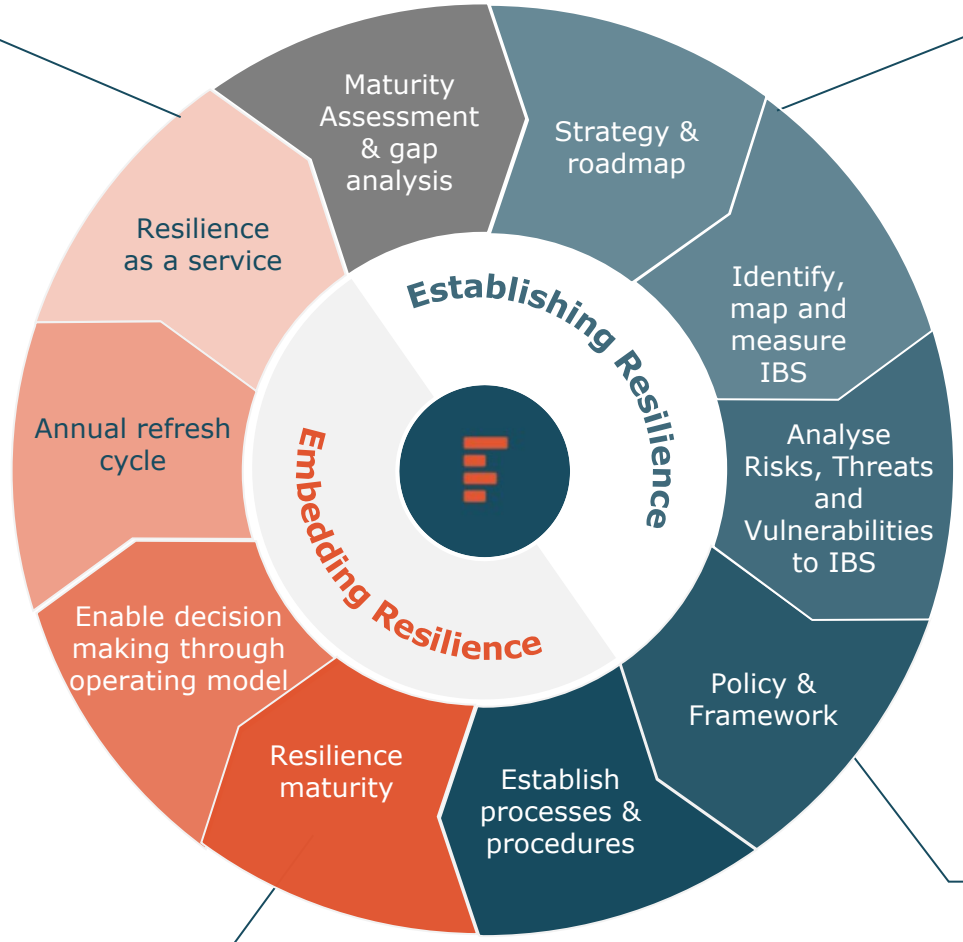
Manage Resilience

Enable the Transfer to management of the resilience framework and associated uplifts through:

- Comprehensive **Management Information Reporting**
- **Target Operating Model design**
- **Enable People** through training & development
- **Build Resilience Capabilities** to respond & recover through recruitment or service provider selection

Develop Resilience

- **Full Remediation Support of resilience gaps,** vulnerabilities identified through 'exposure analysis'
- **Create, Update, Test and Maintain BIAs and Resilience Planning** documentation for 'Important Business Services'.
- **Align Operational Risk Management Capability** – Measurement, Controls, and Procedures
- Develop - **identify, prevent, detect, respond and recover** processes & procedures
- Active Supplier Management



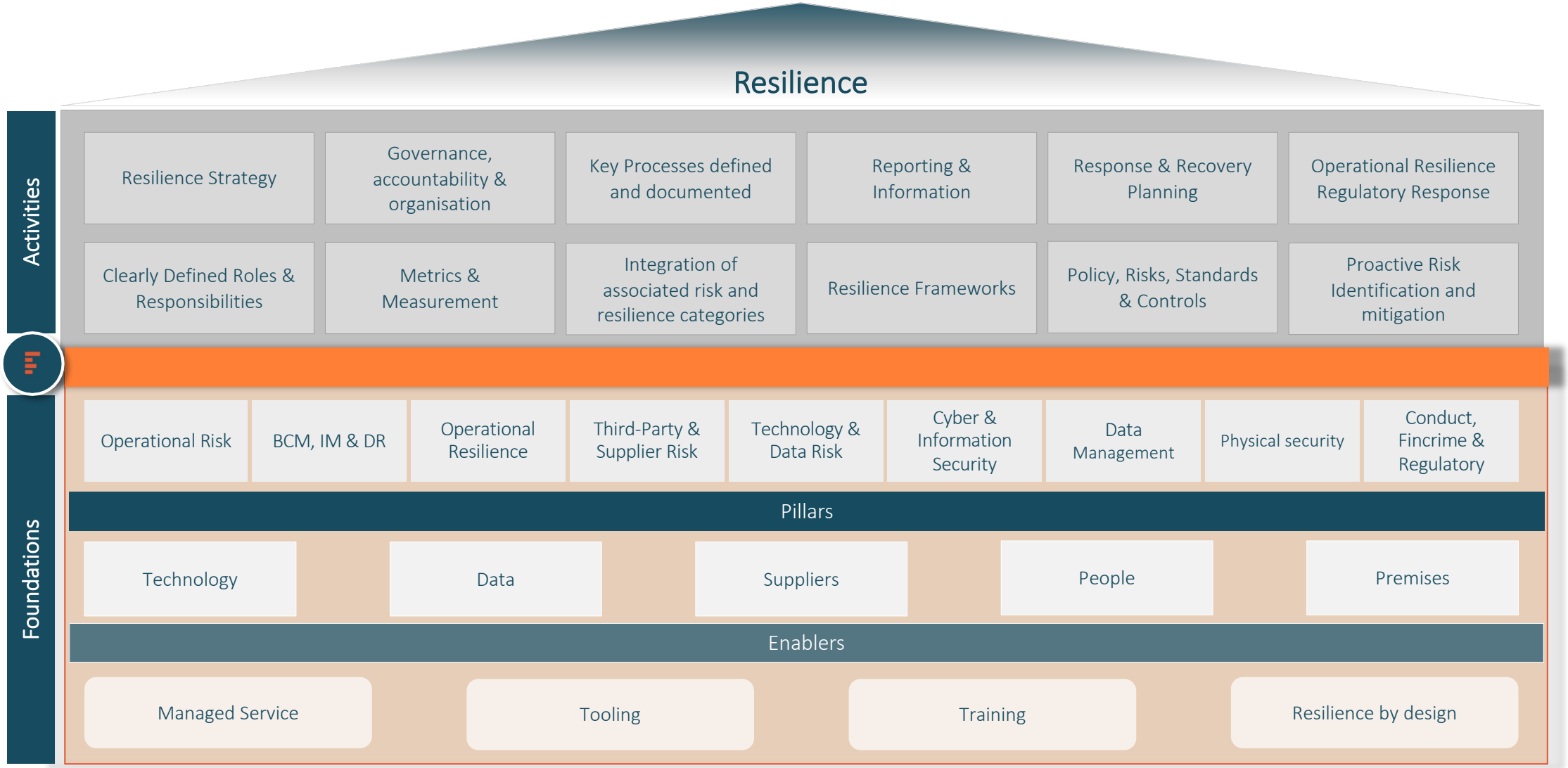
Analyse Resilience

- **Identify, dependency map, and measure Important Business Services through impact tolerances**
- **Resilience Risk Exposure Analysis - Deep Dive Risk Assessment & Measurement of IBS dependent resources**
- **Comprehensive Threats & Vulnerabilities Analysis to form an investment strategy**
- **Identify Library of Scenarios to test ability to respond, recover and communicate during an operational disruption.**

Define Resilience

- **Assess and define desired resilience maturity**
- **Create Future State Vision, Strategy, Appetite & Roadmap that delivers on the desired maturity including transition strategies to test, respond and communicate**
- **Design a Resilience Architecture through the creation of a policy, framework and standards**
- **Design how resilience risk will be controlled through end-to-end processes and procedures**

ACHIEVING RESILIENCE: THE END GOAL



Advisory and Consulting options

FOURTHLINE

OPERATIONAL RESILIENCE GAP ANALYSIS

Objectives

- Carry out a gap analysis of Operational Resilience programme and assess for alignment of existing programme design to regulatory requirements (FCA, PRA, CBI).
- Provide a point in time view of current state Operational Resilience programme design alignment to FCA PS21/3 and/or PRA SS1/21 and/or CBI Operational Resilience regulations.
- Document findings and recommendations which articulate where there are programme design gaps to regulatory requirements and how to remediate those findings.
- Produce a roadmap with an itemised list of required deliverables to meet regulatory requirements.

Technical Scope

- We will assess programme design (e.g. artefacts, playbooks, processes) against FCA PS21/3 Building Operational Resilience, and/or PRA SS1/21 Impact Tolerances for Important Business Services, and/or CBI Cross Industry Guidance on Operational Resilience.

Approach

- Through research and light stakeholder engagement, Fourthline will build an understanding of services and values, products, customers, operating environment and strategy.
- Using our principles-based methodologies we will assess how operational resilience programme design capabilities align with regulatory requirements, through the following steps:
  1. *Submit and RFI for the main Operational Resilience artefacts including policy, mappings, framework, and self-assessment report;*
  2. *Conduct a detailed paper-based review of the received artefacts to determine initial findings and areas to target in stakeholder workshops;*
  3. *On completion of our paper-based reviews and analysis of findings, we will conduct targeted stakeholder workshops to further inform the gap analysis and operationalisation of the programme;*
  4. *We will analyse and finalise all findings to agree on design gaps, operational outcomes and required remediation;*
  5. *FourthLine will produce an Excel workbook with a matrix report highlighting the design capability gaps and summarising recommendations to align with the regulations.*
  6. We will submit the workbook, along with an implementation roadmap and present to interested stakeholders.

Deliverables

- Submitted Excel workbook including:
  - RTM for relevant Operational Resilience regulations
  - Matrix report highlighting the gaps that are required to align with Operational Resilience regulatory requirements and recommendations for creation/uplift
  - A supporting implementation roadmap with an itemised list of required deliverables and action owners
- Present findings and recommendations to interested stakeholders

FourthLine Resources

Client Partner
Senior Resilience Manager
Consultant

Timescale

~4-8 weeks

IMPORTANT BUSINESS SERVICES, MAPPING, IMPACT TOLERANCE SETTING AND SCENARIO TESTING

Objectives

- Identify Important Business Services by determining the intolerable harm that can be caused in the event of a disruption.
- Establish regulatory impact tolerances for each Important Business Service.
- Establish a map of how Important business services are delivered through dependent resources including people, technology, third parties, data, and facilities. Through the mapping process identify vulnerabilities and gaps in resilience capability.
- Finalise resilience assessment by conducting scenario testing using severe but plausible scenarios
- Finalise understanding of vulnerabilities and resilience gaps and update Remediation Plan

Approach

Critical or Important Business Services and Impact Tolerance Setting

1. Through analysis of artefacts, internal functions and services, external products and services, and analysis of the customer journey with products and services we will form a broad view of all potential business services.
2. FourthLine will virtually host a briefing workshop with key stakeholders to discuss: The definition of Important business services; Define intolerable harm to markets, the firm and consumers; Finalise the register of end-to-end business services provided to customers.
3. Using our proprietary Operational Resilience toolkit and methodology, we will virtually host scoring workshops to carry out criticality scoring of selected business services to identify Important business Services.
4. We will capture and document the scored rationale within the FourthLine toolkit and submit a completed toolkit.
5. Present final Important Business Services report to all interested parties and seek approval.
6. We will provide advisory support on the final inclusion and / or exclusion of Important Business Services that Senior Management will take to the board to obtain approval.

Mapping

1. Develop an initial view of the types of threat scenarios that could disrupt Important Business Services.
2. Conduct and document Important Business Services process mapping workshops.
3. Conduct and document resource mapping workshop including integrated Threats and Vulnerabilities Assessment and Resilience Gap Assessment.

Severe but Plausible Scenario Testing

1. Select a severe but plausible (SBP) scenario for testing by completing a risk, impact, likelihood and vulnerability assessment.
2. Stage Scenario Testing workshop focused on 'Impact and Vulnerability' of the SBP scenario.
3. Stage Scenario Testing workshop with technology resource owner to establish existing capabilities to reduce impact of SBP.
4. Stage Scenario Testing workshop with IBS owner to test response, adaptive controls, workarounds, mitigations available to avoid intolerable harm via Impact Tolerance breach, which may be caused by the SBP.
5. Feedback lessons learnt and coaching to all stakeholders involved in the exercise.

Deliverables

- Submitted Excel workbook including:
  - Summary of Important Business Services
  - Supporting rationale for inclusion/exclusion
  - Associated impact tolerance metric
- Completed IBS Process, Dependency and Vulnerability Maps in Visio and Supporting Excel.
- Updated Remediation Plan.
- Testing Strategy, Scenario test report, updated lessons learnt template and self-assessment document.
- Communication Plan.
- Present findings and recommendations to interested stakeholders

FourthLine Resources

Client Partner
Senior Resilience Manager
Consultant

Timescale

~12-16 weeks

FOURTHLINE

OPERATIONAL RESILIENCE GOVERNANCE

Objectives

- Develop the strategy, framework and policy that determines resilience goals and objectives and articulates how to manage and govern Operational Resilience.
- Define the Resilience Risk and support capability controls that enable the production of a current state measurement of Operational Resilience.
- Demonstrate the current state vs target state of resilience against certain severe but plausible scenarios through the production of a point in time metric against each capability.

Approach

Strategy, Policy, Governance, Standards and Controls

- Review all Important Business Services mapping assessments and conduct benchmarking analysis and research to form a view of potential resilience risks impacting Important Business Services relevant to business model.
- Based on research and analysis, design and develop core elements of the Resilience Risk & Controls Framework.
- Stage workshops with stakeholders to assess and analyse the identified resilience risks through to reviewing initial risk treatment strategies.
- Through executive sessions establish objectives and goals for the resilience programme and set an agreed risk tolerance level for Operational Resilience.
- Start documenting the framework (including Resilience Risk Management Plan, Resilience Policy, and Procedures).
- The framework will include accountability, governance model, key roles & responsibilities, framework components, key activities and sequences and more. Seek approval for the established framework designs, so role holders understand responsibilities during the transition from programme to BAU.
- Research and stage internal workshops on the required resilience controls for each resource pillar, i.e., Technology, Facilities, Data, People and Third parties.
- Via workshops or one to one conversations, engage with resource pillar owners to identify and select the right standards and controls against desired maturity which establishes target state of resilience.
- Review of existing Operational Resilience Governance arrangements, committee structures, Terms of Reference to inform conceptual Governance design document.

Resilience measurement

- Complete resilience measurement survey with each resource pillar owner and document gaps / barriers to immediate delivery of target resilience state.
- Analyse the results of the survey, assess resources against immediately achievable controls to produce a point in time current state of resilience.
- Document, present and submit current state vs future state resilience.
- Use the above information to propose updates to 2025 roadmap and investment strategy.

Deliverables

- MS PPT Resilience Risk & Controls Matrix with supporting MS Excel.
- Updated Resilience Risk & Controls Framework document (Plan, Policy and Procedures).
- Operational Resilience Strategy and finalised Remediation Plan.
- Operational Resilience Policy
- Resilience report highlighting current state vs target state of each resource supporting IBS.
- Finalised Resilience Strategy, and Resilience Risk & Control Framework.
- Finalised Resilience Governance Operating Model.

FourthLine Resources

Client Partner
Senior Resilience Manager
Consultant

Timescale

~12-16 weeks

EMBED OPERATIONAL RESILIENCE CAPABILITIES

Objectives

- Embed the Resilience Risk Management Framework through process, and reporting procedure definition.
- Embed the design through the development of an Incident Management process and playbook.
- Embed resilience recovery capabilities through developing Business Continuity and Recovery plans with resource owners to ensure recovery in line with strategy and policy objectives and Impact Tolerances.

Approach

Design and Implement procedures and processes

- Document the Resilience Risk identification and assessment process including provision of criteria methodology.
- Document the Resilience Risk Monitoring, review and reporting process, cycle, frequency, attestation and measurements (KRIs, KPIs)
- Engage with 1st and 2nd line stakeholders to test 1st draft monitoring and reporting process. Include development of detailed procedures based upon reporting information, e.g., Resilience Risk Escalation.
- Finalise procedures and processes ready for submission and approval

Create and embed Response planning

- First draft strawman of tailored response plans based on ICT related failures, develop the criteria that invokes response plans, define the roles and responsibilities and operational procedures that must be followed.
- Engage with 1st and 2nd line stakeholders across resource pillars to test the first draft response plans and ensure stakeholder input into the plans.
- Finalise the plan with a completed ICT Incident and Crisis Management Exercise which tests the developed playbook. Document lessons learnt and feedback to stakeholders.
- Finalise response plan ready for submission and approval.

Create and embed Recovery Planning, and develop resilience culture

- Engage with key stakeholders and raise awareness of the importance of operational resilience framework
- Develop tailored business continuity and recovery plans for each process and/or resource level.
- We will capture outputs from stakeholder workshops, and update resilience recovery documentation. We will organise, schedule and test all business continuity and recovery plans per stated control design.
- We will submit, present and report our findings to leadership team.
- Develop resilience culture activities through firm wide training, and role-based training, aligned with responsibilities in the framework.
- Selection of a resilience tool to manage programme activities.
- Support the activities that focus on the annual programme of activities, framework maintenance, review, continuous improvement.

Deliverables

- Resilience Risk Management procedures and processes
- ICT Incident Management procedures and playbooks to strengthen the capability to respond to disruptive events.
- Tailored Business Continuity Plans for critical processes and/or resources within each Important Business Services
- Tailored Recovery plans for critical processes and/or resources within each Important Business Service
- Completed Firm Wide Training
- Operational Resilience tooling selection

FourthLine Resources

Client Partner
Senior Resilience Manager
Consultant

Timescale

~26 weeks

ENABLEMENT AND ADVISORY

Engagement Model

- Dedicated advisory: 3 sessions each month.
- 1-2 sessions are fixed each month with the third sessions flexible to suit client availability.
- Client is committed to using 3 sessions support each month; the days do not roll over.
- The 3 sessions are a 50/50 balance of client facing activity and offline activity.

Summary of benefits

- Collaborative approach working hand in glove with internal resources and capabilities.
- Continuous knowledge share through dedicated workshops and interactions.
- Provides external validation and provides programme enablement and mentoring to your existing team.
- If more support is needed in a certain period, there is flexibility to increase days.

Overview of FL's retained advisory support responsibilities.

- Our support will be provided through a blend of client-facing activity and offline research, review, check and challenge activity.
- Support the Operational Resilience programme's strategic and tactical decision making, methodology design, strategy development and programme maturity through ad-hoc advisory, and review, check and challenge of artefacts/approach.
- Provide input and guidance to tactical, strategic, implementation and maturity activities.
- Offer opinion on regulatory and regulator outputs and interpretations.
- Training, Coaching and hosting insight sessions for Executive, NEDs, Risk and Resilience stakeholders, CIFs and Pillar owners.
- Attendance at planning sessions / steering meetings / RiskCo / CyberCo.
- Support with stakeholder engagement to influence capability development.
- Providing real time support and guidance in responding to live incidents.

Service Features

- Client has access to a dedicated Senior Manager, and access to a wider team of experts to support different Operational Resilience aspects, as necessary.
- FourthLine will provide a comprehensive Operational Resilience Requirements Traceability Matrix (PS21/3 and SS1/21) linked to programme deliverables to support the service.

Technical Scope

- **In Scope** – Operational Resilience advisory and review, check, challenge activity.
- **Out of Scope** - Programme Design activity, e.g. artefact creation, methodology development, hands-on activity, e.g. mapping, scenario testing, Advising on other operational domains except through their context with Operational Resilience.

Outputs

- Review, check, challenge, advisory with verbal and/or written recommendations on operational resilience related queries, documents and deliverables.
- Delivery of coaching and training.

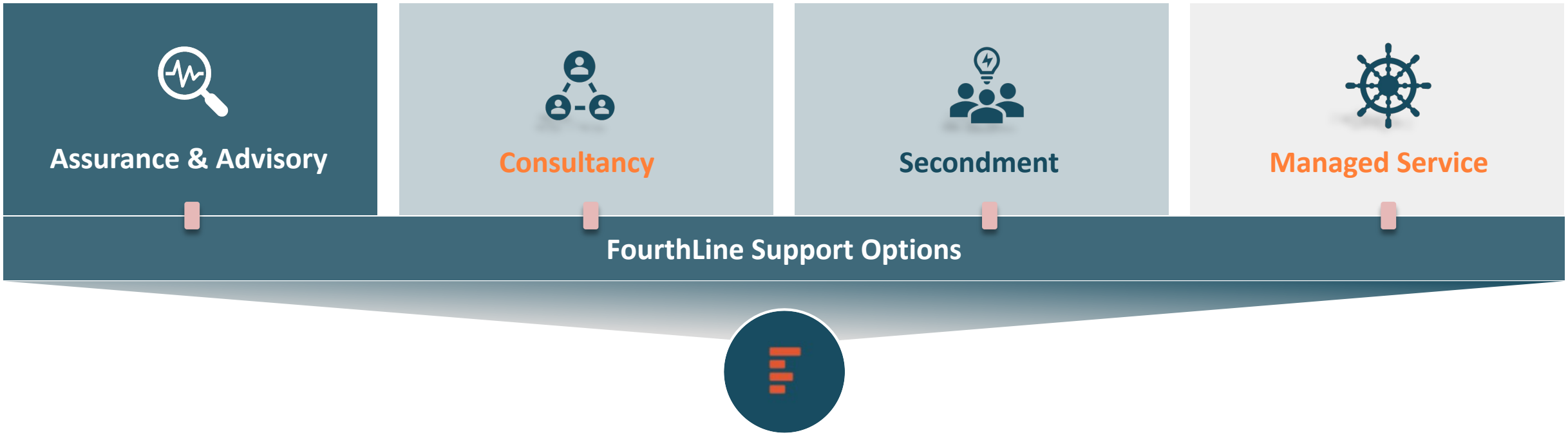
Commercials

- Support provided over a contractual term of 12-months
- 20% mobilisation fee invoiced on agreement of T&Cs.
- Client is committed to using 3 sessions per month.

FourthLine overview

FOURTHLINE

FOURTHLINE – SERVICE OVERVIEW



FourthLine core capability *

- Operational Resilience
- Regulatory & Conduct Risk
- Digital Operational Resilience
- Technology & Data Risk
- Business Continuity
- Crisis & incident Management
- Operational Risk Management
- Information Security & Cyber Risk
- IT Disaster Recovery
- Change Risk & Process Risk
- Product Risk
- Outsourcing & Third-Party Risk

FOURTHLINE – CAPABILITY OVERVIEW

Operational Resilience	Response & Recovery (BCM, ITDR, C&IM)	Third-Party Risk Management	Technology Risk	Regulatory Risk
Important Business Services	Business Impact Analysis	Supplier Risk Assessment	DORA implementation	Consumer Duty
Process, Resource & Dependency Mapping				Product Risk
Threats & Vulnerability Analysis	Recovery Strategies	Materiality Assessment	Change Risk Assessment	Financial Crime*
Establishing Impact Tolerances	Establishing RPOs and RTOs	Supplier Register	IT Criticality Assessment	Client Money and CASS*
Resilience by Design	Threat and scenario analysis	Supplier Testing & Assurance	Critical or Important Functions	Data Protection*
IBS Recovery Plans & Playbooks	Critical Services Matrix	Exit and BCM Planning		Wind-Down Planning*

Current State Assessment / Gap Analysis / Benchmarking / Impact Assessments / Horizon Scanning

Develop programme methodologies

Setting Strategy, Objectives and establishing Risk Appetite

Governance, Framework, Policy, Standard & Controls

KRI / KPI / MI development, Reporting, Template development

Operationalisation through process, procedure and playbook development

Target Operating Model and Framework alignment

Scenario Testing, Crisis and Incident exercising

Tooling Advisory & Implementation

Advisory and BAU Managed Service

CASE STUDIES

Investment Platform

Client`s challenge: Difficulty **in assuring project status** with a clear picture of the outcomes and activities. There were no resources allocated to the program beyond the Lead, plus a lack of executive responsibility with the departure of the COO. Moreover, the client started the work late which coincided with a switch from core to enhanced firm regulation, creating significant urgency. We mobilised quickly and the client achieved compliance by March 22 deadline.

FourthLine approach: We supported the client in the following phases:

1. Important Business Services identification.
2. Important Business Services mapping, creation of a suite of resilience metrics
3. Impact Tolerance setting, scenario creation, testing
4. Self-Assessment

Deposit Taker

Client`s challenge: There was **limited budget** for Operational Resilience. The team was not ready to start the project with limited knowledge and expertise to lead it in-house.

FourthLine approach: We executed an **Enablement approach**, for the client to build enough expertise to run the delivery in-house.

Our approach supported the client with:

1. Board and senior management engagement &project kick off
2. A light Quality Assurance before working through our project phases
3. Important Business Service identification and Vulnerability and Process Mapping
4. Impact Tolerances and Testing
5. Third Party Risk Management review

Pensions and Investments

Client`s challenge: A long term lack of **a risk culture across the firm.** The client had no risk or customer data available and little executive commitment in place. We supported from project inception to project investment steering through delivery. We are working to uplift supporting risk pillars.

FourthLine approach: Delivering an **E2E consultancy** through the following phases:

1. Operational Resilience compliance
2. Risk and Resilience strategy
3. Risk metrics
4. Third Party Risk Management
5. Risk Operating Model
6. Testing, analysis, outline actions

Insurance

Client`s challenge: The client had trebled in size following acquisition and required support for implementing operational resilience and enhancement of supporting frameworks. As a result of the speed of growth, there was little resource capacity and change management capability to deliver a broad programme of work.

FourthLine approach: **E2E Consultancy**

1. Review and Maturity Assessment
2. Operational Resilience regulatory compliance
3. Resilience and investment strategy
4. Resilience Operating Model, Governance and Framework
5. Outsourcing and Third-Party Risk Management

Dan Waltham. Director

daniel.waltham@thefourthline.co.uk

07745780678

Copyright

This content contains copyright © material and trademarks of The FourthLine Ltd.
Copyright © 2022, FourthLine Ltd. All Rights Reserved.

FOURTHLINE