Assessing Business Continuity and IT Disaster Recovery capability

November 2023_v2

FOURTHLINE

BEST PRACTICE APPROACH TO BCM & ITDR PROGRAMMES

Background

The major objective of FCA and PRA Operational Resilience policies is to reduce both the frequency and impact of operational disruptions.

Business Continuity and IT Disaster Recovery capability plays a critical role as the last line of defence in ensuring a firm's overall resilience.

An impact of the new regulations on recovery programmes is the addition of Important Business Services as a factor in assessing response and recovery requirements, such as RTO and RPO.

Those programmes need to adjust to this changing regulatory and operational landscape to maximise the effectiveness of response and recovery planning.

The key issues are:

- Avoiding duplication of effort
- Business Service model alignment
- Understanding the different roles & responsibilities
- Speaking the same language across the programmes
- Understanding the separate testing requirements
- Tooling to support multiple programmes
- Reporting

Leverage Business Service Impact Assessments to inform BCM and ITDR requirements	Define key terms and ensure consistent taxonomy and conduct consistent criticality assessments across all risk disciplines	Mature Risk Management capability with a documented ICT Risk Management framework and robust risk and threat assessment capability
Ensure BCM and ITDR programmes reflect operational realities and likely scenarios	Align IT and Operational incident classification using a criticality matrix linked to the firm's risk impact matrix	Ensure BCM and ITDR policies and playbooks are agile and regularly exercised
Update BCM and ITDR scope, policy and standards to include and align with corporate goals and Operational Resilience	Factoring Important Business Services and Third Parties into testing programmes	BCM and ITDR programme maturity in step with technology capability

BUSINESS CONTINUITY AND ITDR: CHALLENGES

Through our Assessment and Advisory work, we see a wide range of capabilities. Here is an overview of the most common challenges we encounter on client Business Continuity and IT Disaster Recovery programmes.

Informal and undocumented programmes with a heavy focus on a single, onerous and outdated policy not reflective of operational realities

BCM and ITDR programmes lack clear structure and are not aligned to recognised ISO standards or Good Practice Guidance

Lack of integration between BCM and ITDR programmes limits touchpoints, with taxonomies and criticality assessments not aligned

ICT Risk and threat identification is immature or non-existent with no formal IT Risk Management framework in most cases

Poor oversight of critical ICT third-parties response and recovery capabilities creating misalignment with internal initiatives

Recovery priorities, objectives, RPOs and RTOs are set by service owners without an understanding of SLAs or system recovery capability

INDICATIVE OUTLINE OF END-TO-END DELIVERY

Below is a phased delivery approach and example activities and outputs for Business Continuity Management and IT Disaster Recovery.

Phase 1: Assess

- Understand BCM and ITDR capability through a paper-based review and engaging with a sample of stakeholders and Business Continuity Plan owners to assess capability across Organisational context; Leadership; Policy and framework; Roles Responsibilities and Governance; Planning and objectives; Resources and capability; Strategy, Processes, Standards & Controls; Monitoring, Testing and Exercising.
- Draft a gap assessment report with maturity rating and action plan in MS PPT outlining findings and recommendations.
- Draft conceptual BCM and ITDR frameworks, outlining goals, programme regulatory and standards scope, maturity objectives, example people operating models, dependencies and links with other programmes, in-scope systems, processes, departments, products and suppliers
- Mobilise next project phase.

Outputs

- *Comprehensive capability assessment report with an accompanying maturity rating and action plan in MS PPT outlining findings and recommendations for uplifting Business Continuity Management and IT Disaster Recovery, and integration opportunities to enhance approach.*
- *BCM & ITDR frameworks setting the scope and strategy for the programmes.*
- *Undertake a briefing session with project stakeholders to present report findings.*

Phase 2: Plan

- Carry out Business Impact Assessments, Analysis, Risk/Threat Assessments and Criticality Assessments across systems, processes, departments, services, products and suppliers to determine BCM and ITDR operational requirements.
- Determine critical processes, products, services, systems confirming RPO, RTO, MTPD, recovery priorities recovery order for each domain.
- Establish critical matrix outlining critical system recovery capabilities.

Outputs

- *Completed BIA with established MTPD, RPO and RTOs.*
- *Completed risk & threat assessment that informs business continuity solution requirements.*
- *IT DR Criticality Assessment and Matrix.*
- *Completed ICT Risk Assessment.*

Phase 3: Design

- Identify the Business Continuity & IT Disaster Recovery solutions, strategies and measures required to meet RTO, RPO and MTPD to be achieved aligned to the identified criticality requirements from Phase 2
- Develop and document Business Continuity Management and IT Disaster Risk Mitigation strategies (may include a BCP, workarounds, investments).
- Further enhance Business Continuity Management and IT Disaster Recovery methodologies and Recovery strategies as required.

Outputs

- *Documented Business Continuity Management and IT Disaster Recovery Solutions to the identified requirements.*
- *Update to BCM and ITDR framework.*

Phase 4: Implement

- Through client in-house team and / or FourthLine seconded resources:

- Implement Response Structure;
- Develop and manage a Business Continuity Plan(s) for in-scope departments, processes, systems, services;
- Develop and draft a Crisis Management Plan;
- Develop and draft tactical plans and playbooks; aligned to identified risk scenarios;
- Develop and draft operational plans;
- Develop testing and exercising plans.

Outputs

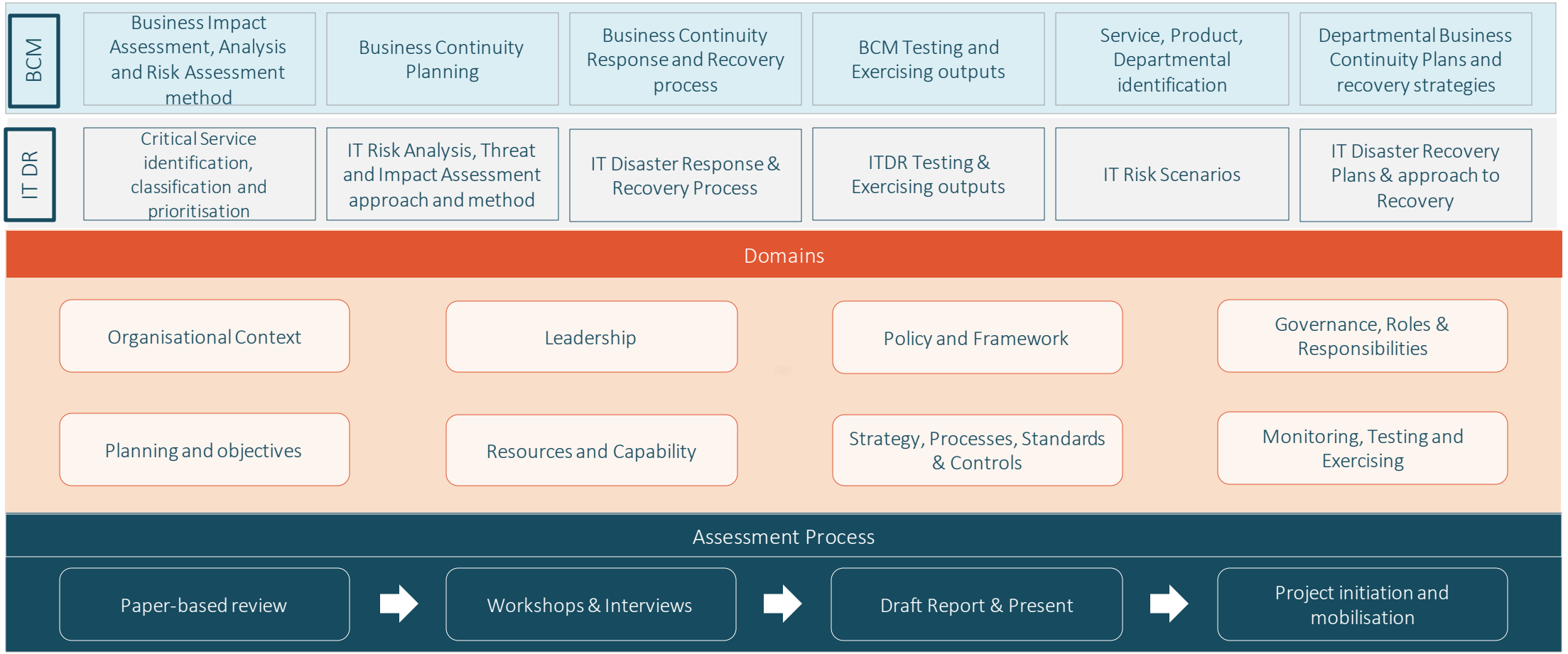
- *Implemented response structure with agreed roles & responsibilities.*
- *Completed and managed Business Continuity Plan for each in-scope department, process, system, service.*
- *Documented Crisis Management Plan including strategic, operational and tactical playbooks.*

ASSESSMENT AND DELIVERY STANDARDS

This is a sample of appropriate regulations and standards that we have previously used to inform and guide good practice for capability assessments in Business Continuity and IT Disaster Recovery.

VISUAL OVERVIEW OF ASSESSMENT AREAS AND PROCESS

Below is a sample of the requirements and domains that make up the Fourthline assessment approach. This has been designed leveraging a combination of; regulatory requirements, good practice, industry standards and years of experience building and managing Business Continuity and Disaster Recovery. The results provide a thorough and broad assessment of capability and effectiveness of capability, highlighting gaps and improvement areas.



ASSESSMENT METHODOLOGY

Below is an example of how we apply our methodology to establish client capability and identify gaps.

Policy & Framework

- Sufficient supporting documents of good quality to managed, govern and respond to incidents, including; Business Continuity Plans, IT Disaster Recovery Plans, BCM and ITDR processes, BCM and ITDR Frameworks, policies, supporting processes and procedures
- Suitably resilient document management system in-place to ensure all associated documents are always available and current from outage / incident inception through to the closure of an outage / incident
- Regular maintenance - review and approval of all documents by senior management ensuring they are current and fit for purpose

Roles, Responsibilities and Governance

- Organisational culture to support the Recovery process
- Reporting on the performance of Business Continuity Management and IT Disaster Recovery
- Leadership and accountability in place at executive level and other relevant management levels
- Adequate governance in-place in the form of well represented committees and forums to support planning, response capability, review of exercises and real-life events

Domains to be assessed

TARGET END STATE

Business Continuity Management and IT Disaster Recovery Capability

Strategy and Objectives

Governance, Reporting and Operating Model

Risk, Impact and Threat Assessment method

Business Continuity Management		IT Disaster Recovery	
Business Continuity Framework	Business Continuity Policy, Standards & Controls	Disaster Recovery Framework	Disaster Recovery Policy, Standards & Controls
Business Continuity Recovery Plans	Roles & Responsibilities	IT Disaster Recovery Plans	Roles & Responsibilities
Business Impact Assessments	Mitigation Methods	Risk Mitigation Strategies	Critical Systems matrix, assessment & tiering method
Recovery Strategies that meet RTO, RPO, MTPD	Business Continuity Recovery Process	IT Disaster Recovery Strategies	IT Disaster Recovery Process
Business Continuity Playbooks	Supporting Processes & Procedures	IT Disaster Recovery Playbooks	Supporting Processes & Procedures

Objectives and Outcomes

Reduce the Business Continuity Management and IT Disaster Recovery risk level ensuring that recovery capability is operational and aligned to industry standards

Establish a proportionate framework, processes and procedures to ensure an effective Business Continuity Management and IT Disaster Recovery approach

Ensure that investment in resilient technologies is supported through a robust Business Continuity Management and ITDR testing and assurance programme

Align Response and Recovery capability to operational resilience and associated disciplines

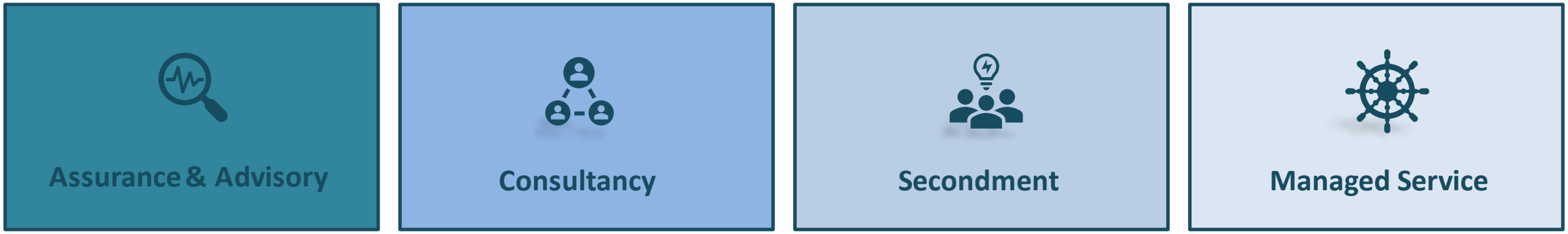
Ensure the approach is understood and embedded throughout the organisation with Playbooks, Exercising, Training and Annual Programme of Activities (APA)

Validation and Maintenance > Exercising and Testing, Training, Annual Programme of Activities (APA)

About FourthLine

FOURTHLINE

YOUR FOURTHLINE OF DEFENCE



FourthLine is a Risk Management and Resilience advisory and consulting firm.

Since 2009, we have supported over 250 UK Financial Services firms with advisory, consulting and resourcing solutions.

We work with clients across non-financial risk domains, including Operational Resilience, Business Continuity, Crisis and Incident Management, IT and Cyber Risk Management, Third-Party Risk Management and Regulatory Risk.

- We close risk and regulatory gaps and uplift frameworks, bringing experience, knowledge, expertise and specialised skills to our client partnerships.
- We help clients achieve and maintain operational effectiveness through proportionate delivery.
- We implement and advise on GRC platforms to improve programme visibility and programme efficiency.
- We provide ongoing risk and resilience support through our contracted service offering.
- We help our clients to become better risk managers, creating the capabilities to achieve risk and resilience maturity.

CORE DELIVERY CAPABILITIES

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 readiness	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 bespoke programme methodologies for in-house delivery

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

Retained Advisory and BAU Managed Service

FOURTHLINE

*Delivered in collaboration with Associate network

OUR DELIVERY PROCESS

Optimise

- Execute the annual cycle of BAU and advisory activities through FourthLine's 12-month managed service contracts.
- Optimise processes & procedures through innovative GRC technology solutions provided by FourthLine's partner network.

Implement

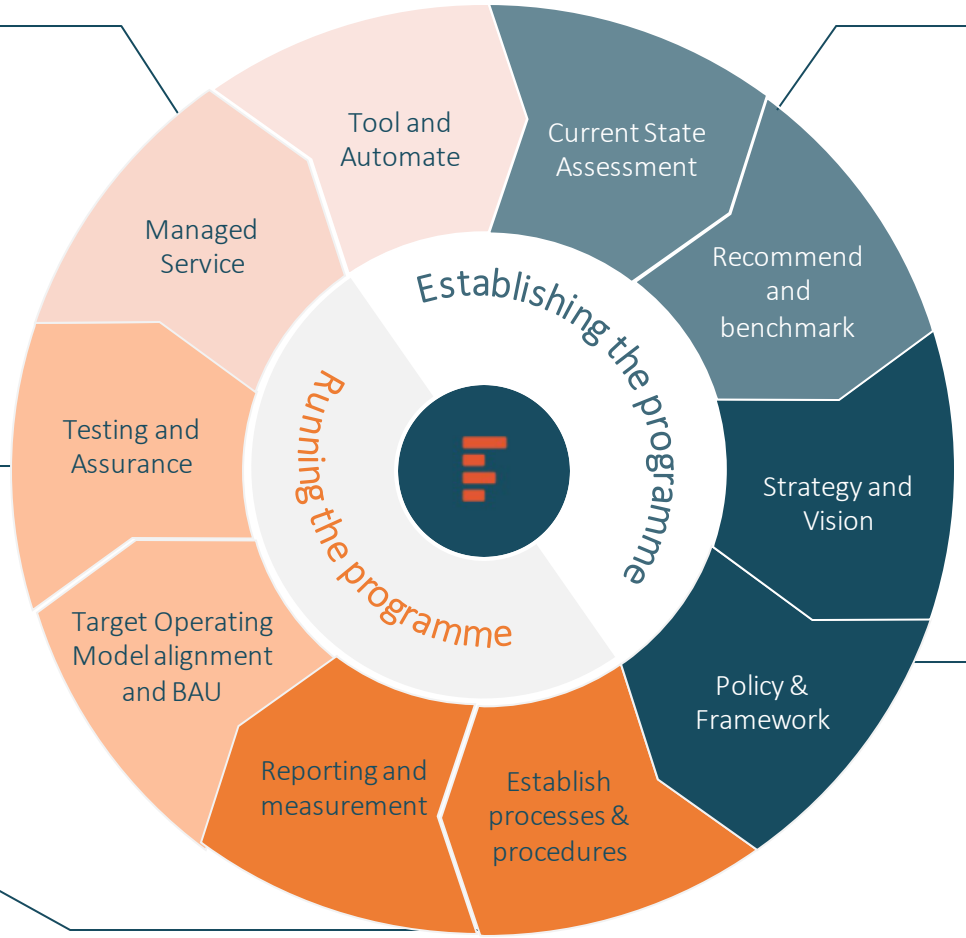
Implement and enable BAU management through:

- Align capability across other risk and protective disciplines through governance, measurement, controls, processes
- Target and People Operating Model design
- Enable People through training & development
- Testing and Assurance of internal capabilities and third-parties

Design

Enable the policy and framework through:

- Design remediation of identified gaps, vulnerabilities identified through current state assessment
- Design and develop comprehensive and active Management Information Reporting
- Design and develop supporting processes & procedures



Understand and Assess

- Understand the firm, operating context, strategy, products, services
- Current State assessment of in-scope capabilities using our principles-based methodology including artefact gap analysis, quality review and stakeholder engagement
- Recommendations for enhancement, uplift and design requirements including maturity score and peer benchmarking

Plan

- Work collaboratively with the organisation to establish the full scope, scale and objectives of the programme
- Create Future State Vision, Strategy, Appetite & Roadmap that delivers on the desired maturity
- Design and document programme methodologies, policy, framework and standards

TEAM CREDENTIALS

Kieran Maplesden (Partner)

- Kieran will act as engagement lead on the GT Bank project, playing a hands-on leadership and operational role throughout.

- Leader of FourthLine's Consulting Operations driving quality output. Kieran is a direct link to our client c-suite and is responsible for governance, steering and escalations
- Currently acting as Client Partner across several engagements linked to Operational Resilience and Business Continuity.
- He has led over 20+ operational resilience and non-financial risk change programmes. Kieran supports clients directly through resilience strategy development, engagement oversight, stakeholder management and engagement governance.
- Kieran acts as overall client partner providing project and resource planning, project review, and service quality monitoring support across each engagement.
- Kieran has 20 years' experience working in professional services in traditional consulting and advisory capacity as well as resource augmentation.

Andrew Voules (Senior Manager)

- Andrew will play the role of Senior Manager, leading on the delivery methodology and acting as our technical design lead.

- Andrew is an Operational Resilience, Technology Resilience and Third-party Risk management expert and an executive level practitioner with 20 years of global experience specialising in the design, implementation and management of Operational Resilience capabilities with cross discipline teams.
- Andrew has led the design and implementation of Operational Resilience capabilities and future operating model in response to new financial regulations (FCA, PRA, BoE) on Operational resilience including improvements across: Important business services (IBS) Outsourcing third party risk management, Business Continuity, Disaster Recovery, Operational Risk, Technology Resilience, Change, MI reporting, Governance, Cyber Risk to gain compliance and achieve and maintain operational resilience.

Taiwo Ojumu (Consultant)

- Taiwo has over 6 years of hands-on experience in BCM and ERM with a proven track record in developing and implementing effective BCM and risk management practices.

- In his Consultant role, Taiwo is currently working with a trading platform to help them identify gaps, and uplift their approaches across Operational Resilience, Business Continuity and IT Disaster Recovery.
- In supporting FL's clients, Taiwo plays a role in workshop leadership, methodology development, capability assessment and documentation.

Amr Elhadd (Consultant)

- MSc graduate in Banking and Finance from Queen Mary University.
- Amr has five years' experience working in financial services for investment, insurance and pensions.

- Amr has a broad skillset with experience across risk, compliance, supplier management, operations and product.
- Amr is currently supporting two investment firms with Operational Resilience maturity programmes.

Dan Waltham. Director

daniel.waltham@thefourthline.co.uk

FOURTHLINE