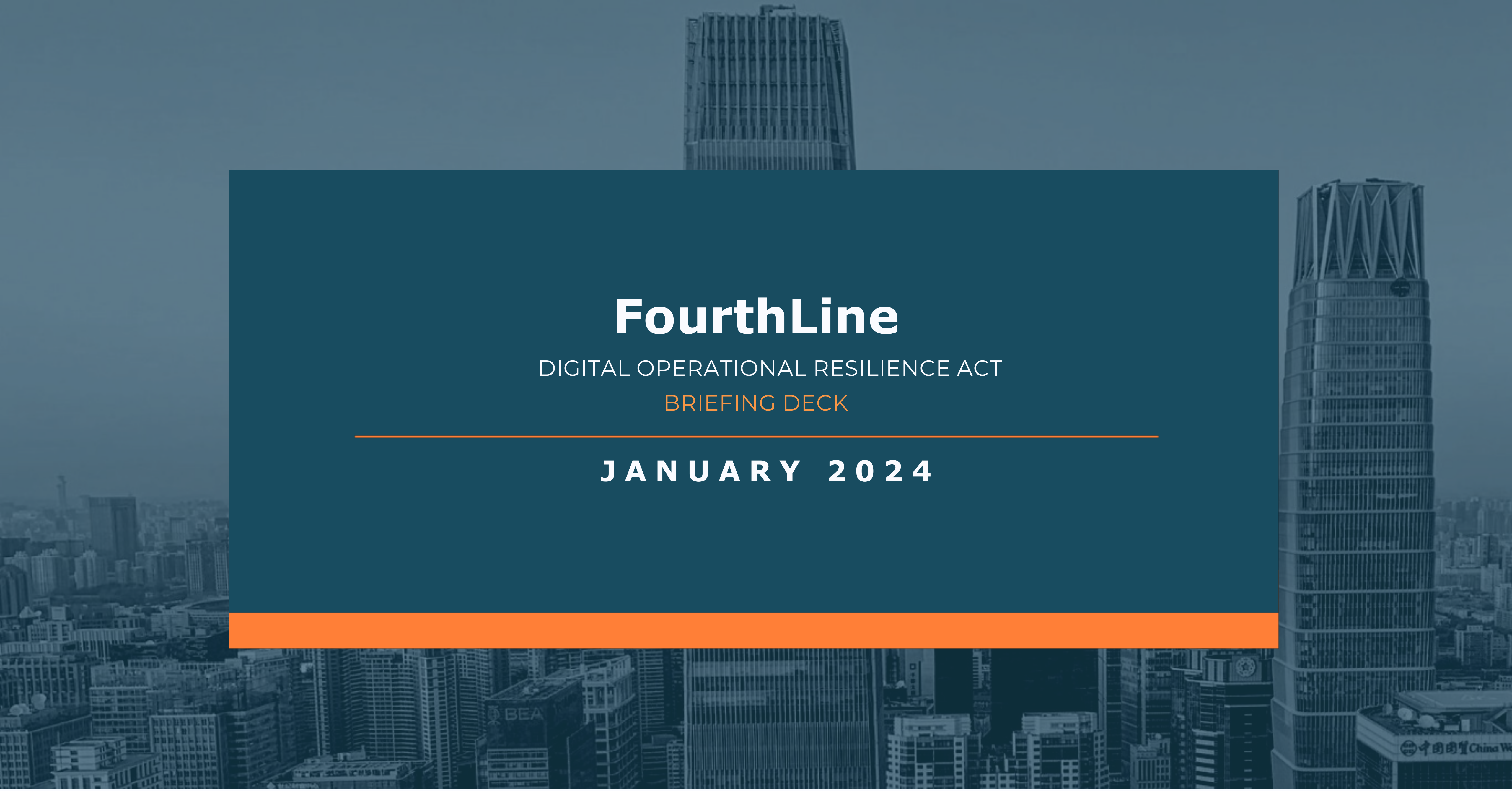


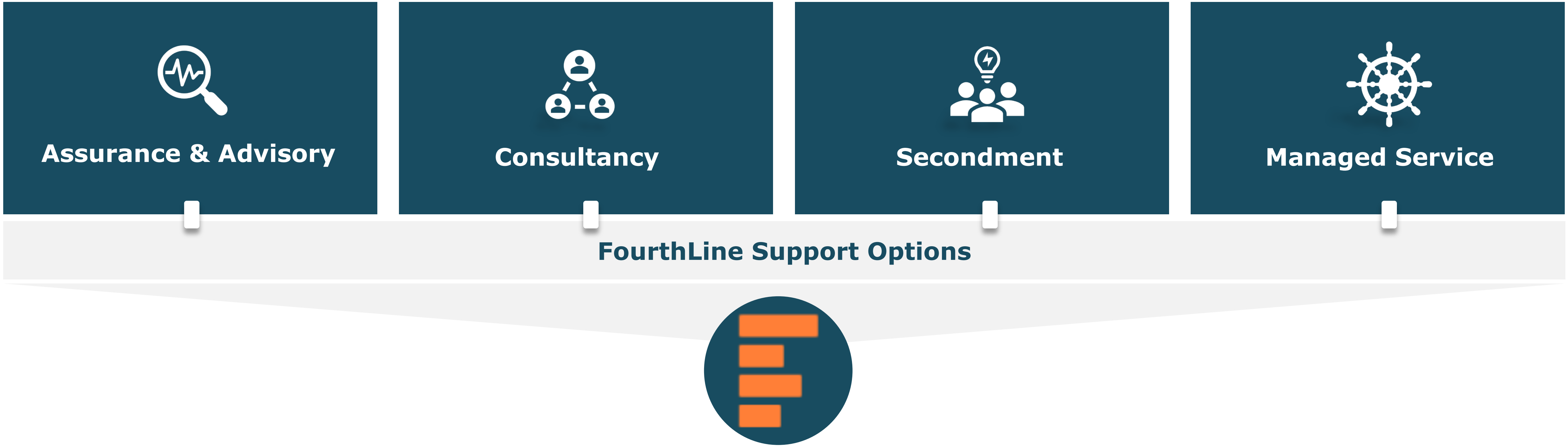
FourthLine

DIGITAL OPERATIONAL RESILIENCE ACT

BRIEFING DECK

JANUARY 2024

FOURTHLINE OVERVIEW



Assurance & Advisory

Consultancy

Secondment

Managed Service

FourthLine Support Options

FourthLine core capability

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

AGENDA

- Background and scope
- DORA framework components
- Selected components and example mapped requirements
- Considerations for framework components
- Suggested Q1 2024 DORA priorities
- Support areas
- Appendix - Selected policy requirements

Definition

Digital Operational Resilience’ is defined by regulators as:

> “*the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*.”

Background

The EC (European Commission) released its Policy articles DORA (Digital Operational Resilience Act) and General Publications Digital Operational Resilience: a challenge for the supervisory community on September 7, 2022.

Giving in-scope firms a two-year implementation period from January 2023 to 17th January 2025, the requirements are set out across several areas, including:

- ICT-related risk management and ICT-related third-party risk management
- Incident Management and reporting of ICT-related incidents
- Contractual agreements concluded between ICT third-party service and financial entities
- Information and intelligence sharing in relation to cyber threats and vulnerabilities
- Digital operational resilience testing
- Minimum technology requirements for firms in-scope

Objectives

- Complementary to existing objectives around financial soundness to ensure that that the financial services sector can maintain resilient operations, thereby protecting services and customers.

- A single approach to supervising 22,000 in-scope firms will create aligned practices across the EU for ICT and cyber resilience.

- Spotlight on strengthening outsourced ICT processes, functions and services.

- Greater information sharing and expectations on regular notification and testing should provide more forward indicators of the threat horizon, allowing the sector to adapt and respond more quickly.

- Synchronisation with global regulators on the concept of resilience.

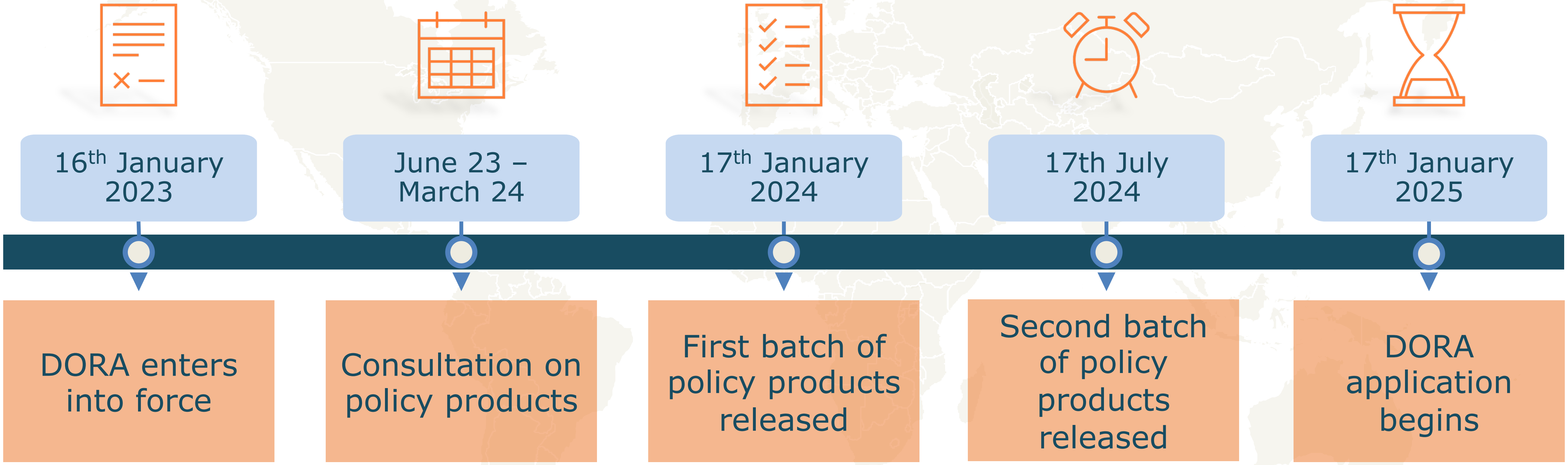
Scope

1. Credit, payment and e-money institutions,
2. Investment firms,
3. Crypto-asset service providers (CASPs) that will be authorised under the Markets in Crypto-Assets Regulation (MiCA) as well as issuers of asset-referenced tokens,
4. Central securities depositories (CSDs),
5. Central counterparties (CCPs),
6. Trading venues,
7. Trade repositories,
8. Alternative investment fund managers (AIFMs),
9. Management companies,
10. Data reporting service providers,
11. Insurance and reinsurance undertakings,
12. Insurance and reinsurance intermediaries,
13. Institutions for occupational retirement pensions,
14. Credit rating agencies,
15. Statutory audit and audit firms,
16. Administrators of critical benchmarks,
17. Crowdfunding service providers,
18. Securitisation repositories.

Proportionality

> *Financial entities shall implement the rules…in accordance with the principle of proportionality, taking into account their size…risk profile, and the nature, scale and complexity of their services, activities and operations*.

TIMELINE



16th January 2023

DORA enters into force

June 23 – March 24

Consultation on policy products

17th January 2024

First batch of policy products released

17th July 2024

Second batch of policy products released

17th January 2025

DORA application begins

OVERALL COMPONENTS OF THE DORA FRAMEWORK

ICT Risk Management	• Governance & Organisation • ICT Risk Management Framework • ICT Systems, Protocols and Tools • Identification • Protection & Prevention • Detection • Response & Recovery • Back Up & Restoration • Learning & Evolving • Communication • Incident Management, Classification & Reporting • Testing
Third-Party Risk Management	• General principles • Concentration Risk • Contractual provisions

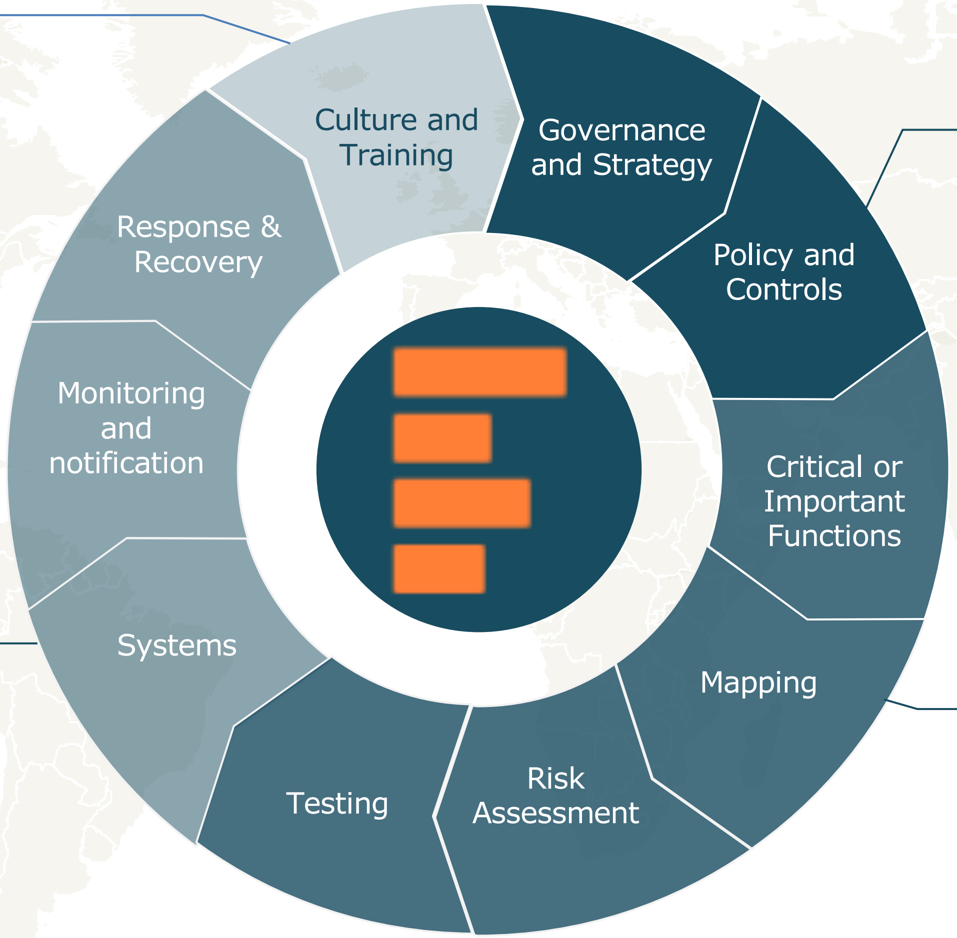
SUMMARY COMPONENTS OF THE DORA FRAMEWORK

Learn

- Digest and build on lessons learned to support ongoing Digital Operational Resilience.
- Develop Security awareness and Digital Operational Resilience training programmes

Respond, Adapt, Recover

- Ensure up to date systems and tools to support resilient ICT estate
- Use continuous monitoring to identify potential threats
- Notify regulators, DORA authorities and peers of threats and major incidents
- Develop a response and recovery capability through Crisis Management, Communications, Business Continuity Management and IT Disaster Recovery



Govern and Manage

- Determine target end state
- Determine responsible owners
- Determine how to manage the programme through appropriate governance, policies, standards and controls
- Supplier arrangements

Identify

- Determine what needs managing through the identification of Critical or Important Functions
- Understand ICT delivery resources and third-party ICT delivery resources across services and functions
- Understand where threats and vulnerabilities exist in those resources
- Test your resilience and recovery capability against severe but plausible scenarios and threats

SELECTED FRAMEWORK COMPONENTS AND MAPPED REQUIREMENTS

Governance and Strategy

Senior management should set "clear roles and responsibilities for all ICT-related functions…establish appropriate governance" and set a "digital operational resilience strategy articulating how the framework shall be implemented"

Outputs: Governance structure, People Operating Model, Strategy and policy governing use of ICT Third-Parties, Updated legal arrangements with suppliers

Policy and Controls

Firms are required to develop a governance and controls framework which ensures "effective and prudent management of ICT risk"

Outputs: ICT Risk Management policy including use of ICT third parties, IT Business Continuity policy, IT Disaster Recovery Policy, Crisis and Communications policy, ICT Risk Management controls, PAM and IAM policies, ICT Ops policy

Critical or Important Functions

Firms are required to understand the functions where failure to deliver, impacted delivery or discontinued delivery would materially impact the safety and soundness of the firm or inhibit the firm's ability to meet the minimum regulatory requirements, e.g., FCA's principles of business.

Outputs: List of Critical or Important functions

Mapping

Firms are required to identify all ICT-related functions and processes and map roles and responsibilities, information and critical ICT assets underpinning those functions and processes.

Outputs: Asset register of all ICT assets supporting a function and map critical assets and key dependencies on third party providers

Risk Assessment

Firms shall "identify all sources of ICT risk, …the risk exposure to and from other financial entities, assess cyber threats and ICT vulnerabilities …of ICT supported business functions, information assets and ICT assets"

Outputs: ICT Risk Assessment and classification, Threats and Vulnerabilities Analysis

Testing

Firms are required to regularly test all capabilities relating to third-party ICT Risk Management including an annual testing programme on legacy ICT and Threat Led Penetration Testing every 3 years as a minimum

Outputs: Controls testing, ITDR, Business Continuity, Crisis and Incident Management testing, Threat-Led Penetration Testing

Monitoring & Notification

Firms must continuously monitor cyber security and ongoing function of ICT systems, develop an incident management notification process which supports early warning indicators and notifies senior management of major incidents.

Outputs: ICT risk monitoring programme, incident notification process

Response & Recovery

Draft and test Business Continuity Plans including Business Continuity & Exit Plans for ICT third partes supporting delivery of Critical or Important Functions

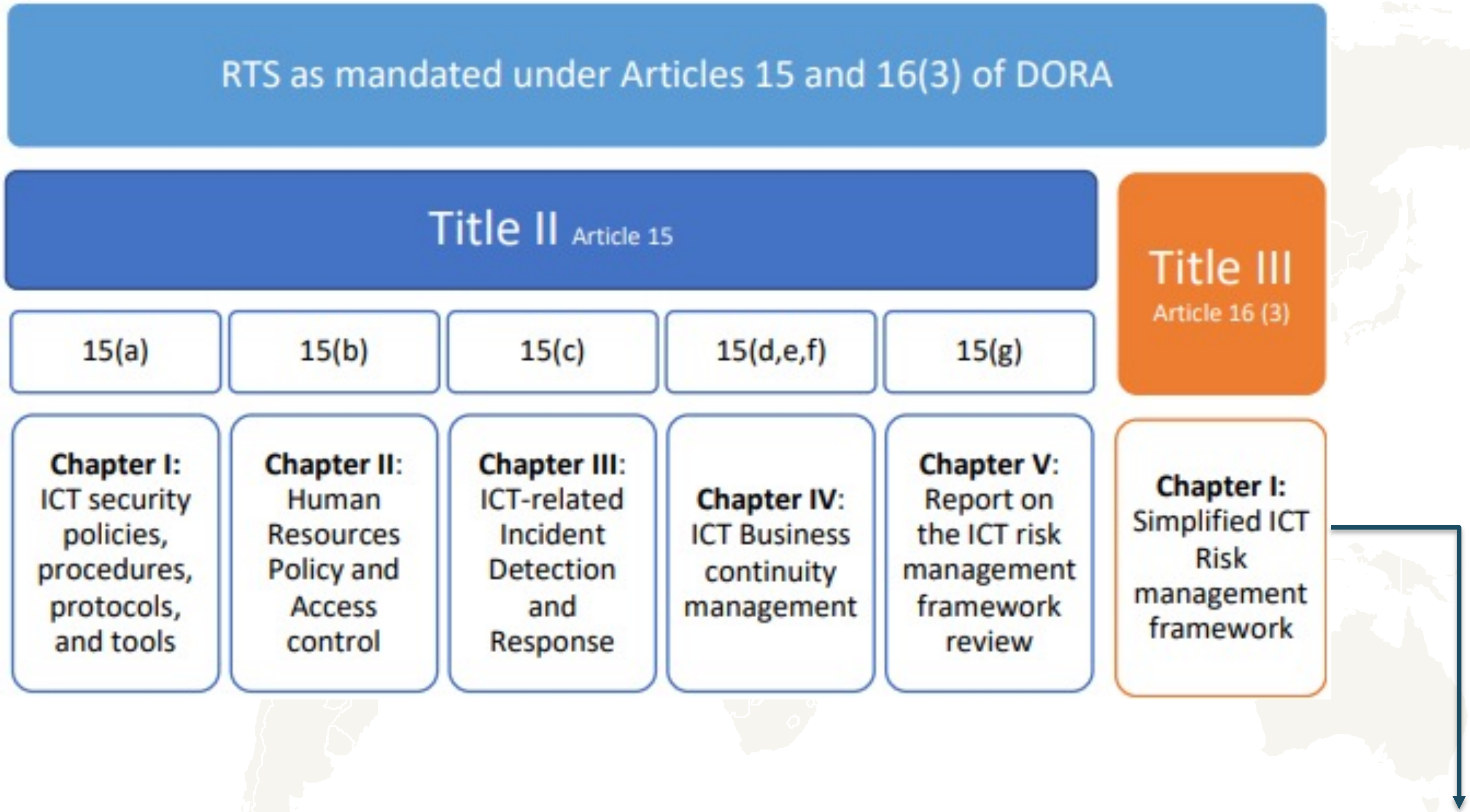
Outputs: Business Impact Assessment, Business Continuity Plans, ITDR Plans, Crisis and Comms Plans

CONSIDERATIONS FOR CRITICAL OR IMPORTANT FUNCTIONS

"A function whose discontinued, defective or failed performance would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services legislation, or its financial performance or the soundness or continuity of its services and activities" (DLA Piper)

- Non-compliance with regulatory obligations and principles for business if unavailable / impaired
- Impacts financial performance if unavailable / impaired
- Impact to safety and Soundness if unavailable / impaired
- Outsourced Control function
- Intended outsourced function requiring regulatory notification
- Functions material to the delivery of Important Business Services
- Services that are essential to the real economy
- Services which would disrupt financial stability if unavailable / impaired
- Lack of substitutability

ICT RISK MANAGEMENT FRAMEWORK REQUIREMENTS



RTS as mandated under Articles 15 and 16(3) of DORA

Title II Article 15

Title III Article 16 (3)

15(a)	15(b)	15(c)	15(d,e,f)	15(g)
Chapter I: ICT security policies, procedures, protocols, and tools	**Chapter II:** Human Resources Policy and Access control	**Chapter III:** ICT-related Incident Detection and Response	**Chapter IV:** ICT Business continuity management	**Chapter V:** Report on the ICT risk management framework review

Chapter I: Simplified ICT Risk management framework

Small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366, institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation, electronic money institutions exempted pursuant to Directive 2009/110/EC, and small institutions for occupational retirement provision

ICT RISK MANAGEMENT FRAMEWORK REQUIREMENTS

Only policies

- ICT Asset Management
- Encryption & Cryptographic controls
- ICT Project Management
- Acquisition, development & maintenance of ICT systems
- Physical and environment security
- Human Resources
- Identity Management
- Access Control
- ICT Incident Management
- ICT Business Continuity

Only procedures

- ICT Asset Management
- Capacity and performance
- Vulnerability and patch management
- Data and systems security
- Logging
- Acquisition, development and maintenance of ICT systems
- ICT Change Management
- Identity Management

Policies and procedures

- ICT Risk Management
- ICT operations
- Network security management
- Security information in transit

“There are in total 20 policies and procedures: in 8 areas only policies are required, in 3 areas specific elements for policies and specific elements for procedures are required, in 5 areas specific elements for procedures and finally in 4 areas policies and procedures are required, without specifying which elements should go in policies and which procedures.“

SUGGESTED CURRENT PRIORITIES

1. Assess current state to identify aligned practice

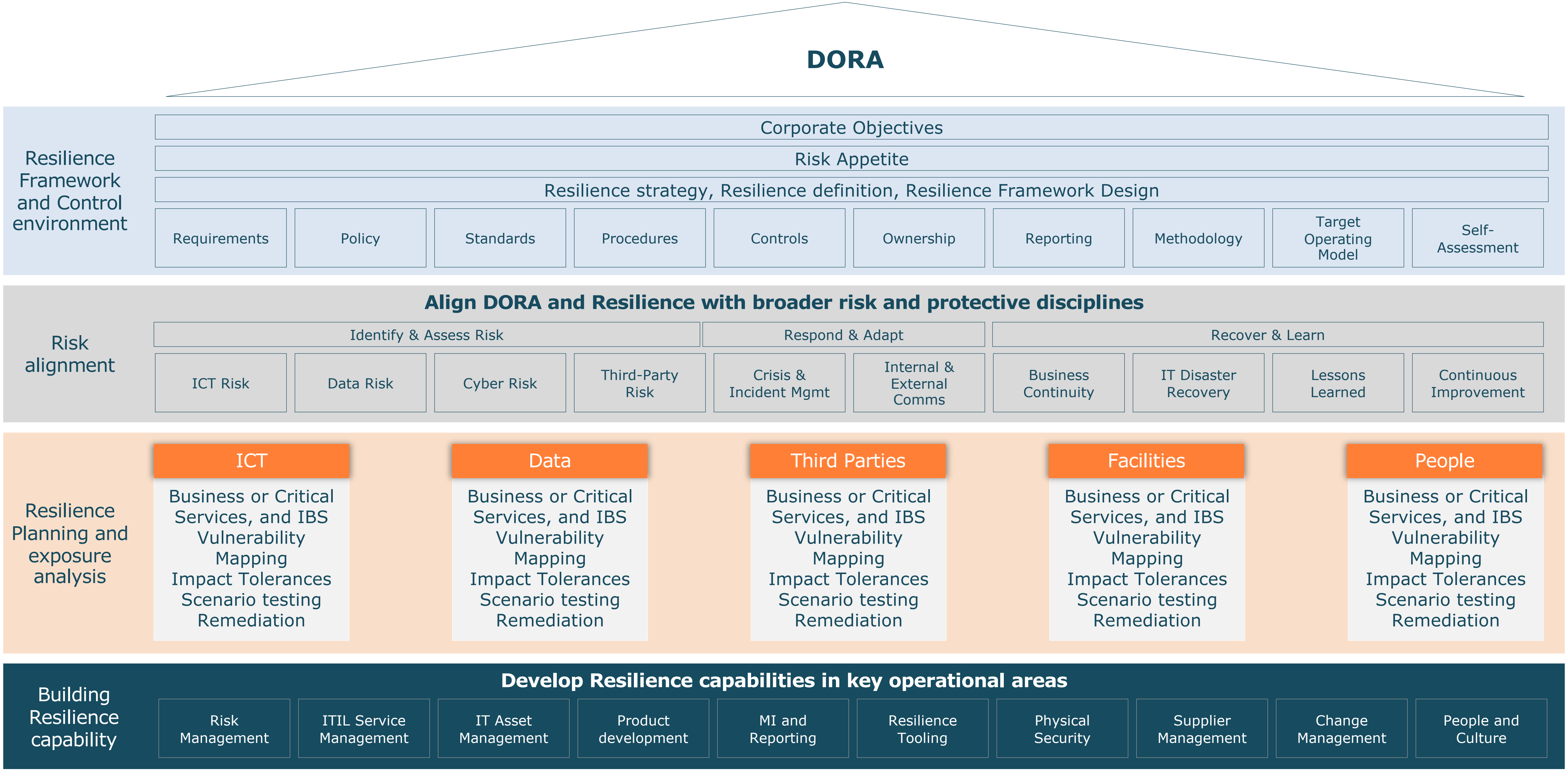
2. Define DORA target state

3. Articulate Digital Operational Resilience Strategy

4. Understand Critical or Important Functions

5. Map ICT Assets

FOURTHLINE’S DORA TARGET STATE



DORA

Resilience Framework and Control environment

- Corporate Objectives
- Risk Appetite
- Resilience strategy, Resilience definition, Resilience Framework Design

Requirements	Policy	Standards	Procedures	Controls	Ownership	Reporting	Methodology	Target Operating Model	Self-Assessment

Risk alignment

Align DORA and Resilience with broader risk and protective disciplines

Identify & Assess Risk				Respond & Adapt		Recover & Learn			
ICT Risk	Data Risk	Cyber Risk	Third-Party Risk	Crisis & Incident Mgmt	Internal & External Comms	Business Continuity	IT Disaster Recovery	Lessons Learned	Continuous Improvement

Resilience Planning and exposure analysis

ICT	Data	Third Parties	Facilities	People
Business or Critical Services, and IBS Vulnerability Mapping Impact Tolerances Scenario testing Remediation	Business or Critical Services, and IBS Vulnerability Mapping Impact Tolerances Scenario testing Remediation	Business or Critical Services, and IBS Vulnerability Mapping Impact Tolerances Scenario testing Remediation	Business or Critical Services, and IBS Vulnerability Mapping Impact Tolerances Scenario testing Remediation	Business or Critical Services, and IBS Vulnerability Mapping Impact Tolerances Scenario testing Remediation

Building Resilience capability

Develop Resilience capabilities in key operational areas

Risk Management	ITIL Service Management	IT Asset Management	Product development	MI and Reporting	Resilience Tooling	Physical Security	Supplier Management	Change Management	People and Culture

Example support options

DORA PROGRAMME DESIGN GAP ANALYSIS

Objectives

- FourthLine to design a DORA gap analysis self-assessment methodology which enables our assessment of gaps to, and design capabilities aligned to DORA regulatory requirements.
- Provide a point in time view of current state DORA programme design alignment to European Supervisory Authorities Digital Operational Resilience Act (2022/2554) and Regulatory Technical Standards (RTS).
- 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 and RTS.

Technical Scope

- We will assess current programme design (e.g. artefacts, playbooks, processes) to identify gaps against European Supervisory Authorities Digital Operational Resilience Act (2022/2554) and Regulatory Technical Standards.

Approach

1. Through research and light stakeholder engagement, Fourthline will finalise engagement scope and build an understanding of services and values, products, customers, operating environment and strategy.
2. We will update our principles-based methodologies to ensure they are proportionate.
3. FourthLine will assess how current programme design meets DORA requirements and where there are gaps to DORA requirements, through the following steps:
   a. *We will provide a questionnaire for DORA leads to complete, enabling us to assess existing programme design alignment to DORA regulations and RTS.*
   b. *Where there are existing artefacts (e.g. policies, frameworks, playbooks, mappings) we will conduct a paper-based review of these artefacts to assess alignment to DORA regulations and RTS.*
   c. *Following analysis of questionnaire responses and artefacts, we will conduct targeted stakeholder workshops to inform our assessment and determine current state design gaps for the ongoing DORA programme.*
   d. *Following completion of workshops, we will finalise all findings, internally agree which design capabilities require remediation or uplift and where there are gaps and design capabilities require creation.*
   e. *FourthLine will produce an Excel workbook with a matrix report highlighting the design capability gaps and summarising recommendations to align with the regulations, and RTS. The Excel document will include a full Requirements Traceability Matrix (RTM) for DORA 2022/2554 and RTS, and an implementation roadmap.*
4. FourthLine will present findings, recommendations, matrix report and roadmap to interested stakeholders.

Deliverables

- Submitted Excel workbook including:
  - Requirements Traceability Matrix for DORA regulations and RTS
  - Matrix report highlighting the gaps that are required to align with DORA regulatory requirements and RTS and recommendations for creation/uplift
  - A supporting implementation roadmap with an itemised list of required deliverables
- Present findings, recommendations, roadmap to interested stakeholders.

FourthLine Resources

Client Partner
Senior Manager
Consultant

Timescale

6 – 8 weeks following mobilisation

IDENTIFY CRITICAL OR IMPORTANT FUNCTIONS AND MAP ICT ASSETS

Objectives

- Using our proprietary methodology, FourthLine will research all functions and lead the business through a series of workshops to identify and score Critical or Important functions (CIFs) for prioritisation during DORA implementation.
- FourthLine will map and classify all ICT Assets, making determinations for criticality for those assets supporting CIFs and identify process and resource flow and dependencies to create detailed mapping and ICT Asset Register artefacts.
- FourthLine will Conduct ICT Risk, Threats & Vulnerabilities Assessment of all critical ICT Assets.

Approach

Identify

1. Through analysis of artefacts, internal functions and services, external products and services , we will form a broad view of all functions.
2. Through online research, artefact review, and stakeholder workshops, FourthLine will build a Service Asset Catalogue which documents all ICT resources, ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk.
3. Further assessment will be conducted to ensure that all information assets and ICT assets, including those on remote sites, network resources and hardware equipment are captured in the Service Asset Catalogue.
4. FL will virtually host a briefing workshop with stakeholders to discuss the definition of Critical or Important Functions and finalise the register of E2E business services.
5. Using FL methodology, we will virtually host scoring workshops to carry out criticality scoring of selected business services to identify CIFs
6. Capture and document the scored rationale within the FL toolkit and submit a completed toolkit.
7. FL to provide advisory on the final inclusion and / or exclusion of CIFs that Senior Management will take to the board to obtain approval.
8. Present final CIF report and Service Asset Catalogue to interested parties and gain client approval.

Classify

1. Develop an initial view of the types of threat scenarios that could disrupt Critical or Important Functions (CIFs)
2. Conduct mapping workshops for CIFs identifying and document all processes, including those dependent on ICT third-party providers, identifying interconnections with ICT third-party service providers that provide services that support critical or important functions
3. Conduct and document CIF resource mapping workshops including integrated TVA and Resilience Gap Assessment.
4. Using process and resource mapping and BIAs / ITDR Classifications / IT Risk assessment classifications / CIF identification as reference tools, through targeted stakeholder workshops and offline analysis, determine which ICT Assets contained in the Service Asset Catalogue are considered "critical" to client operations, functions and services
5. Once "critical" ICT Resources have been determined and documented, gain client approval
6. For critical ICT assets, FourthLine to further map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets
7. Present final phase report, Critical Asset log and furtner mapping to interested parties and gain client approval

Threats & Vulnerabilities Assessment (TVA)

1. Using information gathered in the integrated TVA and Resilience Gap Assessment (Classify: Step 3), FourthLine to review and analyse alongside CIF mapping to document initial findings on threats and vulnerabilities to ICT resources.
2. Where required, conduct follow up workshops with targeted stakeholders to gather further information on ICT resources, ICT Third-parties and potential threats and vulnerabilities to support findings.
3. Complete initial draft of TVA and present to interested parties.
4. Final draft of TVA, presented via a remediation investment plan in MS Word.

Deliverables

- Service Asset Catalogue which lists all ICT resources, ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk
- List of Business functions, internal and external services
- Documented and approved list of Critical or Important Functions
- End to end process and resource mapped CIFs presented in MS Visio
- Completed Threats & Vulnerabilities Assessment presented via a DORA Investment Plan in MS Word
- List of Critical ICT Assets presented in a Critical Asset log updated in the Service Asset Catalogue

FourthLine Resources

Client Partner
Technology Resilience Senior Manager
Consultant

Timescale

~12-16 weeks following mobilisation

TAILORED DORA STRATEGY & FRAMEWORK DOCUMENT

Objectives and Technical scope

- We will develop digital resilience strategy and ICT Risk framework documents, tailored to ICT architecture and objectives. The framework will include accountability, governance model, key roles & responsibilities, framework components, key activities of the DORA programme and the strategy will articulate how you will achieve the framework objectives.
- Both the framework and strategy will meet DORA regulations and articulate the overall aims of the DORA programme, providing a combined blueprint to move from current state to target state.
- **Technical scope**: DORA regulation, framework & strategy articles, aligned to DORA 2022/2554 requirements & Regulatory Technical Standards.

Approach

Establish current state, strategy and framework document (10 weeks)

1. Understand current ICT architecture, standards and stated requirements across all aspects of the ICT operating environment including suppliers, data centres, internal applications etc that leads to the articulation of 'current state' requirement within the **DORA strategy document.**
2. Through data analysis, we will develop an understanding of the ICT Risk Management performance from risk data, previous incidents and the effectiveness of preventative measures in place that will inform an updated ''current state' within the **DORA strategy document**.
3. Use the organisational objectives and ICT strategy objectives to align risk categories which will be used for the ICT risk assessment.
4. Through executive sessions establish risk tolerance level for ICT risk and using the risk impact matrix set an ICT risk tolerance threshold.
5. Establish the **ICT Risk Management Framework Document** including Plan, Policy and Procedure definition. The framework will include accountability, governance model, key roles & responsibilities, framework components, key activities and sequences and more.
6. Seek approval for the established framework designs, so role holders understand responsibilities during the transition from programme to BAU.
7. Point review of IS framework and engage with CISO to establish view on information security objectives, performance indicators and risk metrics.
8. Establish current state vs future state vision, and DORA architecture explaining the methods / standards / procedures for creation or development.
9. Update, present and obtain approval for **DORA Framework document**.

DORA Design and ICT Risk Assessment (8 weeks)

1. Through understanding of organisation and ICT objectives conduct a series of interviews and off-line research with ICT Service owners to identify scenarios and events that could impact objectives.
2. Assess the causes, consequences and likelihood of each event identified and take the highest rated risks and assess and evaluate existing controls and treatment options that aim to prevent and protect, detect, respond and recover.
3. Summarise findings in an **ICT Risk Assessment report**.

Develop digital operational resilience strategies (8-10 weeks)

1. Following review of the ICT reference architecture template, develop digital resilience strategies and changes required to improve resilience which may include duplicate processing across systems, modular redundancy, inherent resilience by design and automatic fault tolerance within systems.
2. Produce and agree digital resilience testing plan, and procedural methodology through collaboration with ICT service owners. Ensure the testing plan is based upon the unique threats, vulnerabilities faced by your organisation and delivers appropriate outcomes.
3. Based upon severe ICT related incidents that lead to crisis & incident management conduct a series of table-top scenario tests that aims to assess internal and external communication requirements. Develop the communication strategy following the test, engage and obtain approval.
4. Following the ICT Risk Assessment conclusions develop Digital Resilience Standards and controls suite of documentation that aligns with NIST / DORA RTS that inform how ICT risk will be addressed and objectives met.
5. Update, present and obtain approval for final **DORA Strategy document**.

Deliverables

- In-depth ICT Risk Assessment and associated report
- Submitted and approved ICT Risk Management Framework document
- Submitted and approved DORA strategy, tailored to ICT architecture
- Present to interested stakeholders and gain final approval.

FourthLine Resources

Client Partner
Technology Resilience Snr Manager
Consultant

Timescale

~30 - 32 weeks following mobilisation

DORA 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.

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 DORA 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 DORA planning sessions / steering meetings / RiskCo / CyberCo.
- Support with stakeholder engagement to influence DORA capability development.
- Providing real time support and guidance in responding to live incidents.

Outputs

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

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.

Service Features

- Client has access to a dedicated Senior Manager, and access to a wider team of experts to support different DORA requirements, as necessary.
- FourthLine will provide a comprehensive DORA Requirements Traceability Matrix linked to programme deliverables to support the service.

Technical Scope

- **In Scope** – DORA implementation Advisory and review, check, challenge activity with scope specifically focused on GRC (non-technology) aspects.
- **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 DORA

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

Appendix: DORA RTS policy requirements

DORA: GOVERNANCE AND CONTROLS

1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.
2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1). For the purposes of the first subparagraph, the management body shall:
   - (a) bear the ultimate responsibility for managing the financial entity’s ICT risk;
   - (b) put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;
   - (c) set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;
   - (d) bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);
   - (e) approve, oversee and periodically review the implementation of the financial entity’s ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity’s overall business continuity policy and response and recovery plan;
   - (f) approve and periodically review the financial entity’s ICT internal audit plans, ICT audits and material modifications to them;
   - (g) allocate and periodically review the appropriate budget to fulfil the financial entity’s digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff; 27.12.2022 EN Official Journal of the European Union L 333/29
   - (h) approve and periodically review the financial entity’s policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;
     - (i) put in place, at corporate level, reporting channels enabling it to be duly informed of the following:
     - (i) arrangements concluded with ICT third-party service providers on the use of ICT services,
     - (ii) any relevant planned material changes regarding the ICT third-party service providers,
     - (iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.
3. Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.
4. Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.

DORA: ICT RISK MANAGEMENT FRAMEWORK: STRATEGY

1. The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:
   (a) explaining how the ICT risk management framework supports the financial entity’s business strategy and objectives;
   (b) establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;
   (c) setting out clear information security objectives, including key performance indicators and key risk metrics;
   (d) explaining the ICT reference architecture and any changes needed to reach specific business objectives;
   (e) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;
   (f) evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;
   (g) implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;
   (h) outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT RISK POLICY

1. The indication of the approval of the risk tolerance level for ICT risk established according to Article 6(8), point (b), of Regulation (EU) 2022/2554;
2. the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators to measure impact and likelihood of those vulnerabilities being exploited by threats;
3. the procedure to identify, implement and document ICT risk treatment measures for the ICT risk assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance levels referred to in point (a). The procedure shall ensure the monitoring of the effectiveness of the measures implemented, the assessment of whether the established risk tolerance levels of the financial entity have been attained and that the financial entity takes actions to correct or improve the measures where necessary;
4. with reference to the ICT risk that is still present following the implementation of the ICT risk treatment measures:
   (i) provisions on the identification of residual ICT risks;
   (ii) the assignment of roles and responsibilities regarding the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level referred to in point (a), and for the assessment process referred to in point (iv);
   (iii)the development of an inventory of the accepted residual ICT risks, including an explanation of the reasons for which they were accepted;
   (iv)provisions on the assessment of the accepted residual ICT risks at least once a year, including the identification of any changes to the residual ICT risks, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the review;
5. provisions on the monitoring of any changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk of the financial entity to promptly detect changes that could affect its ICT risk profile
6. provisions on a process to ensure that changes to the business strategy and the digital operational resilience strategy of the financial entity, if any, are taken into account.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ASSET MANAGEMENT POLICY

1. require the monitoring and management of the life cycle of ICT assets identified and classified in accordance with Article 8(1) of Regulation (EU) 2022/2554;
2. require the financial entity to keep records of all of the following:
    I. unique identifier of each ICT asset;
    II. information on the location, either physical or logical, of all ICT assets;
    III. the classification of all ICT assets, as specified in Article 8(1) of Regulation (EU) 2022/2254;
    IV. the identity of ICT asset owners;
    V. business functions or services supported by the ICT asset;
    VI. the ICT business continuity requirements, including recovery time objectives and recovery point objective;
    VII. whether the ICT asset may be or is exposed to external networks, including the internet;
    VIII. the links and interdependencies among ICT assets and the business functions using each ICT asset;
    IX. where applicable, for all ICT assets, the end dates of the ICT third-party service provider's regular, extended and custom support services after which it is no longer supported by its supplier or by an ICT third-party service provider;
3. for financial entities referred to in Article 8(7) of Regulation (EU) 2022/2554, prescribe that they keep records of the information needed to perform a specific ICT risk assessment on all legacy ICT systems.

Asset Management Procedure

1. Financial entities shall develop, document and implement an ICT asset management procedure, with a view to preserving the availability, authenticity, integrity and confidentiality of data.
2. Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. The assessment shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities of the financial entity

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT OPERATIONS POLICY

1. As part of the ICT security policies and procedures, financial entities shall develop, document and implement policies and procedures to manage the ICT operations of ICT assets, with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data. These policies and procedures shall define how financial entities operate, monitor, control and restore their ICT assets, including the documentation of ICT operations.

2. The policies and procedures for ICT operations referred to in paragraph 1 shall include all of the following elements:
   - (a) ICT assets description, including all of the following: (i) secure installation, maintenance, configuration and deinstallation of ICT systems; (ii) management of information assets used by ICT assets, including their processing and handling, automated and manual; (iii)identification and control of legacy ICT systems;
   - (b) controls and monitoring of ICT systems, including all of the following:
     - (i) backup and restoration requirements of ICT systems;
     - (ii) scheduling requirements, taking into consideration interdependencies among the ICT systems;
     - (iii) protocols for audit-trail and system log information;
     - (iv) requirements to ensure that the performance of internal audit and other testing minimises disruptions to business operations;
     - (v) requirements on the separation of ICT production environments from the development, testing and other non-production environments. The separation shall consider all of the components of the environment, such as accounts, data or connections;
     - (vi) requirements to conduct the development and testing in environments which are separated from the production environment;
     - (vii) requirements to conduct the development and testing in production environments. The policies and procedures shall provide that the instances in which testing is performed in production environment are clearly identified, justified, for limited periods of time approved by the relevant function, and considering Article 16(6). The availability, confidentiality, integrity and authenticity of ICT systems and production data shall be ensured during development and test activities in production environment;
   - (c) error handling concerning ICT systems, including all of the following:
     - (i) procedures and protocols for handling errors;
     - (ii) support and escalation contacts, including external support contacts in case of unexpected operational or technical issues;
     - (iii) ICT system restart, rollback and recovery procedures for use in the event of ICT system disruption.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT PROJECT MGMT POLICY

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement an ICT project management policy.
2. The ICT project management policy shall define the elements to ensure the effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the financial entity’s ICT systems.
3. 3. The ICT project management policy shall include all of the following elements:
   (a) project objectives;
   (b) project governance, including roles and responsibilities;
   (c) project planning, timeframe and steps;
   (d) project risk assessment;
   (e) relevant milestones;
   (f) change management requirements;
   (g) testing of all requirements, including security requirements, and the respective approval process when deploying an ICT system in the production environment.
4. The ICT project management policy shall ensure the secure ICT project implementation through the provision of the necessary information and expertise from the business area or functions impacted by the ICT project.
5. The ICT project management policy shall provide that the establishment and progress of ICT projects impacting critical or important functions and their associated risks shall be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, periodically and, where necessary, on an event-driven basis, in accordance with ICT project risk assessment included in paragraph 3, point (d).

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT SYSTEMS POLICY

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy **governing the acquisition, development and maintenance of ICT systems**. This policy shall:
   (a) identify security practices and methodologies relating to the acquisition, development and maintenance of ICT systems;
   (b) require the identification of technical specification and ICT technical specification, as respectively defined in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012, of requirements relating to acquisition, development and maintenance of ICT systems, with a particular focus on ICT security requirements and on their approval by the relevant business function and ICT asset owner according to the financial entity's internal governance arrangements;
   (c) define measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development, maintenance and deployment in the production environment.
2. Financial entities shall develop, document and implement an ICT systems' acquisition, development and maintenance procedure, which shall include all of the following:
   (a) the requirements to test and approve all ICT systems prior to their use and after maintenance, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). The level of testing shall be commensurate to the criticality of the concerned business functions and ICT assets. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally.
   (b) the requirements to perform source code reviews covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and 61 applications, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation.
   (c) the requirements to perform security testing of software packages at no later than the integration phase, in accordance with Article 8(2), point (b), points (v), (vi) and (vii).
   (d) the requirement that non-production environments only store anonymized, pseudonymized or randomized production data and that financial entities shall protect the integrity and confidentiality of data in non-production environments.
   (e) the requirement to implement controls to protect the integrity of the source code of ICT systems that are developed in-house or by an ICT third-party service provider and delivered to the financial entity by an ICT third-parties service provider;
   (f) the requirement that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment.
3. For the purposes of the testing according to paragraph 2, point (a):
   (a) central counterparties shall involve, as appropriate, in the design and conduct of these tests, clearing members and clients, interoperable central counterparties and other interested parties;
   (b) central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in its business continuity policy.
4. By way of derogation from paragraph 2, point (d), production data that are not anonymized, not pseudonymized or not randomized may be stored only for specific testing occasions, for limited periods of time and following the approval by the relevant function and, for financial entities other than microenterprises, the reporting of such occasions to the ICT risk management function.
5. The procedures referred in this Article shall also apply to ICT systems developed or managed by users outside the ICT function, using a risk-based approach.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT CHANGE MGMT POLICY

1. As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement ICT change management procedures.
2. Financial entities shall include in the ICT change management procedures, in respect of all changes to software, hardware, firmware components, systems or security parameters, all of the following elements:
   (a)verification that ICT security requirements have been met;
   (b)mechanisms to ensure independence between the functions that approve changes and those responsible for requesting and implementing them;
   (c)definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is an effective quality assurance;
   (d)documentation and communication of change details, including purpose and scope of the change, the timeline for implementation and the expected outcomes;
   (e)identification of fall-back procedures and responsibilities, including procedures and responsibilities for aborting changes or recovering from changes not successfully implemented;
   (f)procedures, protocols and tools to manage emergency changes that provide adequate safeguards;
   (g)procedures to document, re-evaluate, assess and approve after their implementation emergency changes, including workarounds and patches;
   (h)identification of the potential impact of a change on existing ICT security measures and assessment of whether it requires the adoption of additional ICT security measures.
3. After making significant changes to its systems, central counterparties and central securities depositories shall submit their ICT systems to stringent testing by simulating stressed conditions:
   (a)a central counterparty shall involve, as appropriate, in the design and conduct of these tests: clearing members and clients, interoperable central counterparties and other interested parties;
   (b)a central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in its ICT business continuity policy.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: HR POLICY

1. As part of their human resource or other relevant policies financial entities shall include all of the following ICT security related elements:
   (a) identification and assignment of any specific ICT security responsibilities;
   (b) requirements for staff of the financial entity and of the ICT third-party service providers using or accessing ICT assets of the financial entity to:
      (i) be informed about, and adhere to, the financial entity's ICT security policies, procedures and protocols;
      (ii) be aware of the reporting channels put in place by the financial entity for the purpose of detection of anomalous behaviour, including, where applicable, those established according to Directive (EU) 2019/1937 of the European Parliament and of the Council16;
      (iii) upon termination of employment, requirements for the staff to return to the financial entity all ICT assets and tangible information assets in their possession that belong to the financial entity.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT INCIDENT MGMT POLICY

1. As part of the mechanisms to detect anomalous activities, including ICT network performance issues and ICT-related incidents, financial entities shall develop, document and implement an ICT-related incident policy through which they shall:
   (a) document the ICT-related incident management process referred to in Article 17 of Regulation (EU) 2022/2554;
   (b) establish a list of relevant contacts with internal functions and external stakeholders that are directly involved in ICT operations' security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management;
   (c) establish, implement and operate technical, organisational and operational mechanisms to support the ICT-related incident management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours in accordance with Article 23;
   (d) retain all evidence relating to ICT-related incidents for a period no longer than necessary for the purposes for which the data is collected, commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets, in accordance with [Article [15] of Commission Delegated Regulation (EU) […]/[…] [Commission Delegated Regulation on classification of ICT-related incidents] and with any applicable retention requirement according to Union law. This evidence shall be retained in a secure manner.
   (e) establish and implement mechanisms to analyse significant or recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: ICT INCIDENT CRITERIA

1. Financial entities shall set clear roles and responsibilities to effectively detect and respond to ICT-related incidents and anomalous activities.
2. To detect anomalous activities, ICT network performance issues and ICT-related incidents in accordance with Article 10(1) of Regulation (EU) 2022/2554, financial entities shall implement detection mechanisms allowing them to:
   - (a)collect, monitor and analyse all of the following:
     - (i) internal and external factors, including at least the logs collected according to Article 12, information from business and ICT functions and any problem reported by users of the financial entity;
     - (ii) potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity;
     - (iii) ICT-related incident notification from an ICT third-party service provider of the financial entity detected in the ICT systems and networks of the ICT third-party service provider and which may affect the financial entity;
   - (b)identify anomalous activities and behaviour and implement tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and the integrity of the data sources or log collection;
   - (c)prioritise the alerts referred to in point (b) to allow the detected ICT-related incidents to be managed within the expected resolution time, as defined by financial entities, both during and outside working hours;
   - (d)record, analyse and evaluate any relevant information on all anomalous activities and behaviours automatically or manually.
3. Any recording of the anomalous activities shall be protected against tampering and unauthorised access at rest, in transit and, where relevant, in use.
4. The financial entity shall log all relevant information for each detected anomalous activity to enable identification of the date and time of occurrence and detection, and the type of the anomalous activity.
5. Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes:
   - (a)indications that malicious activity may have been carried out in an ICT system or network or that such ICT system or network may have been compromised;
   - (b)data losses detected, in relation to the availability, authenticity, integrity and confidentiality of data;
   - (c)adverse impact detected on financial entity's transactions and operations;
   - (d)ICT systems' and network unavailability.
6. When evaluating the criteria set out in paragraph 5, financial entities shall consider the criticality of the services affected

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: BC POLICY

1. Financial entities shall include in their ICT business continuity policy all of the following:
   - (a) definition of the objectives, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA) referred to in Article 11(5) of Regulation (EU) 2022/2554;
   - (b) definition of the scope, including limitations and exclusions, to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;
   - (c) definition of the timeframe to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms;
   - (d) description of the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans and crisis communications plans;
   - (e) provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the ICT business continuity policy and to ensure that sufficient resources are available;
   - (f) provisions on the alignment between the ICT business continuity plans and the overall business continuity plans. The alignment shall concern at least all of the following: (i) potential failure scenarios, including those listed in Article 26(2); (ii) recovery objectives, specifying that the financial entity shall be able to recover the operations of its critical or important functions after disruptions within a recovery time objective and a recovery point objective;
   - (g) provisions on the development of ICT business continuity plans for severe business disruptions as part of these plans, and the prioritisation of ICT business continuity actions using a risk-based approach;
   - (h) provisions on the development, testing and review of ICT response and recovery plans, in accordance with Articles 25 and 26;
   - (i) provisions on the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26;
   - (j) provisions to align the ICT business continuity policy to the communication policy referred to in Article 14(2) of Regulation (EU) 2022/2554 and to the communication and crisis communication actions referred to in Article 11(2), point (e), of Regulation (EU) 2022/2554.
2. In addition to the requirements referred to in paragraph 1, central counterparties shall ensure that their ICT business continuity policy:
   - (a) includes a maximum recovery time for their critical functions that is not higher than two hours. End of day procedures and payments shall be completed on the required time and day in all circumstances;
   - (b) takes into account external links and interdependencies within the financial infrastructures including trading venues cleared by the central counterparty, securities settlement and payment systems and credit institutions used by the central counterparty or a linked central counterparty;
   - (c) requires that arrangements are in place to: (i) ensure the continuity of their critical or important functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions and fail over and recovery to a secondary site; (ii) maintain a secondary processing site capable of ensuring continuity of their critical or important functions identical to the primary site. The secondary processing site shall have a geographical risk profile which is distinct from that of the primary site; (iii)maintain or have immediate access to a secondary business site to allow staff to ensure continuity of the service if the primary location of business is not available; (iv)consider the need for additional processing sites, in particular if the diversity of the risk profiles of the primary and secondary sites does not provide sufficient 71 confidence that the central counterparty's business continuity objectives will be met in all scenarios.
3. In addition to the requirements referred to in paragraph 1, central securities depositories shall ensure that their ICT business continuity policy:
   - (a) takes into account any links and interdependencies to at least users, critical utilities and critical service providers, other central securities depositories and other market infrastructures;
   - (b) requires its ICT business continuity arrangements to ensure that the recovery time objective for their critical or important functions shall not be longer than two hours.
4. In addition to the requirements referred to in paragraph 1, trading venues shall ensure that their ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any ICT service of the trading venue after a disruptive incident is close to zero.

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: BUSINESS CONT. TESTING

1. Financial entities shall test the ICT business continuity plans taking into account the financial entity’s BIA and the ICT risk assessment referred to in Article 3(1), point (b).
2. Financial entities shall assess through the testing of their ICT business continuity plans whether they are able to ensure the continuity of the financial entity’s critical or important functions. The testing of the ICT business continuity plan shall:
   (a) be performed on the basis of test scenarios that simulate potential disruptions, including an adequate set of severe but plausible scenarios. The scenarios considered for the development of the business continuity plans shall always be included in the testing;
   (b) include the testing of ICT services provided by ICT third-parties service providers, where applicable. In testing the business continuity plans as regards ICT third-parties services, financial entities shall duly consider scenarios linked to insolvency or failures of the ICT-third party service provider or of political risks in the provider’s jurisdiction, where relevant;
   (c) for financial entities referred to in the second subparagraph of Article 11(6) of Regulation (EU) 2022/2554, include scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities. The testing shall 72 verify whether at least critical or important functions can be operated appropriately, for a sufficient period of time and whether the normal functioning may be restored;
   (d) be designed to challenge the assumptions on which the business continuity plans rest, including governance arrangements and crisis communication plans;
   (e) include procedures to verify the ability of the staff of financial entities, ICT third party service providers, ICT systems and ICT services to respond adequately to the scenarios duly taken into account in Article 26(2).
3. In addition to the requirements referred to in paragraph 2, for central counterparties the testing of their ICT business continuity plans shall include the involvement of clearing members, external providers and relevant institutions in the financial infrastructure with which interdependencies have been identified in their business continuity policies.
4. In addition to the requirements referred to in paragraph 2, for central securities depositories the testing of their ICT business continuity plans shall include the participation of, as appropriate, users of the central securities depositories, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in their business continuity policy.
5. Test results shall be documented and any identified deficiencies resulting from the tests shall be analysed, addressed and reported to the management body

DORA RTS: ICT RISK MANAGEMENT FRAMEWORK: RESPONSE & RECOVERY PLANS

1. Financial entities shall develop ICT response and recovery plans taking into account the results of the BIA. The ICT response and recovery plans shall:
   (a) specify the conditions prompting their activation, deactivation and any exceptions;
   (b) describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least ICT systems and services supporting critical or important functions of the financial entities;
   (c) be designed to meet the recovery objectives of the operations of the financial entities;
   (d) be documented and made available to the staff involved in their execution and be readily accessible in case of emergency. Financial entities shall clearly define roles and responsibilities to that extent;
   (e) provide for both short-term and long-term recovery options including partial systems recovery;
   (f) lay down the objectives and the conditions to declare a successful execution of the plans.
2. The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. Financial entities shall duly take into account all of the following scenarios:
   (a) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities;
   (b) scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly consider the potential impact of the insolvency or other failures of any relevant ICT third-party service provider;
   (c) partial or total failure of premises, including office and business premises, and data centres;
   (d) substantial failure of ICT assets or of the communication infrastructure;
   (e) the non-availability of a critical number of staff or staff members in charge of guaranteeing the continuity of operations;
   (f) impact of climate change and environment degradation related events, natural disasters, pandemic, and physical attacks, including intrusions and terrorist attacks;
   (g) insider attacks;
   (h) political and social instability, including, where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed;
   (i) widespread power outages.
3. The ICT response and recovery plans shall consider alternative options where the primary recovery measures may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.
4. As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers of ICT services supporting critical or important functions to the financial entity

Daniel Waltham
Director, FourthLine

M: 0774 5780 678
E: daniel.waltham@thefourthline.co.uk

Disclaimer
All content in this document is provided to you by The FourthLine Ltd, which is a limited company registered in England, with a registered office at Arkwright House, Parsonage Gardens, Manchester, M3 2LF

The information contained in this document is of a general nature and is not intended to address the circumstances of any individual or entity. Although FourthLine will endeavour to provide timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on the information in this document without appropriate professional advice after a thorough examination of the particular situation. No entity at The FourthLine Ltd shall have any responsibility or owe any duty to any person in respect of this content; or be responsible for any loss whatsoever sustained by any person who relies on this content.